Maryland Law Review

Volume 82 | Issue 4 Article 2

Prescribing Exploitation

Charlotte A. Tschider

Recommended Citation

Charlotte A. Tschider, *Prescribing Exploitation*, 82 Md. L. Rev. 857 ()
Available at: https://digitalcommons.law.umaryland.edu/mlr/vol82/iss4/2

PRESCRIBING EXPLOITATION

CHARLOTTE A. TSCHIDER[*]

Patients are increasingly reliant temporarily, if not indefinitely, on connected medical devices and wearables, many of which use artificial intelligence ("AI") infrastructures and physical housing that directly interacts with the human body. The automated systems that drive the infrastructures of medical devices and wearables, especially those using complex AI, often use dynamically inscrutable algorithms that may render discriminatory effects that alter paths of treatment and other aspects of patient welfare.

Previous contributions to the literature, however, have not explored how AI technologies animate exploitation of medical technology users. Although all commercial relationships may exploit users to some degree, some forms of health data exploitation exceed the bounds of normative acceptability. The factors that illustrate excessive exploitation that should require some legal intervention include: (1) existence of a fiduciary relationship or approximation of such a relationship, (2) a technology-user relationship that does not involve the expertise of the fiduciary, (3) existence of a critical health event or health status requiring use of a medical device, (4) ubiquitous sensitive data collection essential to AI functionality, (5) lack of reasonably similar analog technology alternatives, and (6) compulsory reliance on a medical device.

This Article makes three key contributions to the existing literature. First, this Article establishes the existence of a type of exploitation that is not only exacerbated by technology but creates additional risk by its ongoing use. Second, this Article illustrates the need for cross-disciplinary engagement between privacy scholarship and AI ethics scholarship, both of which could balance data collection for fairness and safety with other

[*] I would like to thank Professors Sharona Hoffman, W. Nicholson Price, II, Rachel Sachs, Ryan Calo, Sue Glueck, Brian Holland, Saurabh Vishnubhakat, Glynn Lunney, Peter Yu, Doron Dorfman, Ana Santos Rutschman, BJ Ard, Hannah Bloch-Webha, Matthew Sipe, Sara Gerke, Anya Prince, Myrisha Lewis, Christa Laser, my Loyola University Chicago School of Law faculty colleagues, and my excellent research assistant Marisa Polowitz for their helpful suggestions throughout the development of this Article. I would also like to thank the *Maryland Law Review* editorial staff, especially Luca Artista, for their excellent suggestions and care in editing this Article. A very special thank you to Dr. Krista Kennedy, my collaborator and friend, for the extensive conversations leading to this Article.

individual interests. This Article then illustrates how a modern information fiduciary model could neutralize patient exploitation risk when exploitation exceeds normative bounds of community acceptability.

INTRODUCTION

Patients are increasingly reliant temporarily, if not indefinitely, on connected medical devices and wearables, many of which use artificial intelligence ("AI") infrastructures and physical housing that directly interacts with the human body. The automated systems that drive the infrastructures of connected medical devices, especially complex AI, often use dynamically inscrutable algorithms that exploit patients and may render discriminatory effects that alter paths of treatment and other aspects of patient welfare.[1]

Scholarly contributions have scrutinized immediate and potentially harmful automated decisional effects on marginalized communities and groups, based on characteristics such as race, ethnicity, religion, gender, sexual identity, or disability status and proxies for these characteristics.[2] This valuable research, however, has not examined how artificial intelligence actually exacerbates exploitation—that is exploitation based on substantial and pervasive loss of privacy.[3] Exploitation is the process of using a human for your own ends, discussed in relation to commercial financial benefit.[4] Although exploitation to some extent is unavoidable based on power and information disparities, exploitation may exceed our social norms, making it excessive. As this Article aims to illustrate, exploitation may be *excessive* related to personal information when the cumulative effect of power differentials, trust deficiencies, and opacity, concerns that have occupied privacy and algorithmic fairness literature for some time, exceed U.S. social norms.

This exploitation results from a combination of factors essential to effective medical device AI operation that nevertheless make an individual almost exclusively reliant on a health care organization[5]:

[1] Jenna Wiens, W. Nicholson Price II & Michael W. Sjoding, *Diagnosing Bias in Data-Driven Algorithms for Healthcare*, 26 NATURE MED. 25, 25–26 (2020).

[2] Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671, 675 (2016); Anya E.R. Prince & Daniel Schwarcz, *Proxy Discrimination in the Age of Artificial Intelligence and Big Data*, 105 IOWA L. REV. 1257, 1268–69 (2020).

[3] *See infra* text accompanying notes 179–185.

[4] Nicholas Vrousalis, *Exploitation: A Primer*, 13 PHIL. COMPASS, Feb. 2018, at 1.

[5] It should be noted that although this Article focuses on the healthcare sector, the exploitation of the individual is not unique to healthcare. Exploitation may present itself differently

(1) Existence of a fiduciary relationship or approximation of a fiduciary relationship that gives the appearance of expertise and trust;

(2) A technology-user relationship that does not involve the expertise of the fiduciary, as is frequently the case in AI technologies that doctors do not fully understand;[6]

(3) Existence of a critical health event or health status requiring the use of a medical device;

(4) Compulsory use of a medical device;

(5) Lack of reasonably similar technology alternatives, limiting options in controlling data about oneself; and

(6) Ubiquitous sensitive data collection essential to AI functionality and corresponding AI opacity.[7]

Each of these factors, and especially the cumulative combination of such factors, increases the probability of exploitation, a deontological privacy risk resulting from excessive data collection and use.[8] When patients reliant on medical device AI are disproportionately and unreasonably exposed to substantially more privacy risk than their peers, their potential exploitation must be subject to reasonable preventative steps. If individuals who are compulsorily dependent on AI-enabled healthcare technologies are uniquely vulnerable relative to their non-technology-dependent peers, organizations should owe additional duties to mitigate such risks to an acceptable level.

Consider the following example:

> *Gildas has worn a hearing aid for most of their life, since experiencing a labyrinthine concussion from an explosion while growing up during the Second Congo War. When Gildas moved with their family to the United States, Gildas received their first hearing aid, but the first hearing aid amplified all of the environmental sounds, causing serious ringing and pain for Gildas. Gildas has used a masking device instead of a hearing aid*

in different commercial sectors and between different types of actors, for example, as between the government and those accused or convicted of crimes. This Article aims to illustrate how excessive exploitation results in disproportionate burdens on a portion of the population, and further burdens those already burdened by the invisible structures that perpetuate discrimination.

[6] For example, complex AI systems created by manufacturers will not likely be understandable to a doctor, who is in a fiduciary relationship of trust with their patient. The doctor is required to act with a duty of care, but the patient may have implanted technologies where the manufacturer communicates with the patient and the doctor is not involved. In both cases, the doctor's ability to provide a duty of expertise, duty of care, and duty of loyalty is severely limited because the manufacturer is actually providing the treatment. However, a manufacturer does not have any existing fiduciary duty to the individual. The patient may assume that the device is safe and effective because a doctor prescribes it, a fiduciary, but this trust is misplaced.

[7] *See infra* Parts III, IV.

[8] W. Nicholson Price II & I. Glenn Cohen, *Privacy in the Age of Medical Big Data*, 25 NATURE MED. 37, 37–40 (2019).

> *most of their life, but Gildas' hearing never returned, causing serious issues in Gildas' education and opportunities. Gildas recently started college, and after meeting with their physician, Gildas became aware of a new AI-enabled hearing aid that could mask or amplify certain sounds to help Gildas hear their professors' lectures more easily.*[9]

At first glance, this is a feel-good story: A patient will receive a medical device that will transform their learning experience. However, upon closer inspection, the patient is likely exposed to a substantial privacy risk. The doctor or an audiologist likely does not know how data from the patient are used by an AI hearing aid and cannot explain these practices in detail to the patient. Examples of the data collected include environmental and location data, identities of the patients' contacts, and even the patient's music playlist, helpfully integrated within the hearing aid app on their mobile device.[10] These data are transferred as identifiable personal information along with a wide variety of other lifestyle data to manufacturer systems.[11]

Although the features of such a product may be knowable, the ways in which the product makes decisions about the wearer are not.[12] Many AI systems have hidden layers and complex algorithms that likely cannot be easily explained, to physicians or to patients.[13] The substantial volumes of data collected to create and later run these AI systems may be transferred to additional third parties, such as a cellular provider, mobile device manufacturer, or data collated between users and sold to data brokers.[14] What meaningful choice does Gildas have?

As a result of data collection for an arguably necessary and continuously wearable medical device, Gildas will be rendered a digital approximation of themself, datafied, disembodied, and potentially subject to data overuse.[15] Gildas may also be subject to greater *consequentialist* risk, such as impersonation and fraud, and unauthorized access or disclosure of their

[9] This scenario is based on a recent study that involved mapping information ecologies for hearing devices. *See* Krista Kennedy, Noah Wilson & Charlotte Tschider, *Balancing the Halo: Data Surveillance Disclosure and Algorithmic Opacity in Smart Hearing Aids*, 4 RHETORIC HEALTH & MED. 33, 43, 65 (2021) (describing the data protection issues with hearing aids).

[10] *Id.*; STARKEY, LIVIO (2020), https://starkeypro.com/pdfs/livio/livio_patient_brochure.pdf.

[11] *See* Kennedy et al., *supra* note 9, at 43–46.

[12] Thomas Grote & Philipp Berens, *On the Ethics of Algorithmic Decision-Making in Healthcare*, 46 J. MED. ETHICS 205, 208 (2020). The lack of transparency within AI system decisions impacts shared decision-making between physician and patient, decisions that may necessarily include questions of data use as well as medical decisional risks and benefits. *Id.*

[13] U.S. FOOD & DRUG ADMIN., ARTIFICIAL INTELLIGENCE (AI) AND MACHINE LEARNING (ML) IN MEDICAL DEVICES 4, 9 (2020), https://www.fda.gov/media/142998/download.

[14] *See* Kennedy et al., *supra* note 9, at 43–45.

[15] See *infra* Section II.D, describing datafication and the natural tendency to remove the "personal" from personal information in large data sets.

sensitive data.[16] If Gildas is already subject to discrimination based on Gildas' status and identity, exploitation of Gildas' personal information may multiply or exacerbate existing discriminatory effects.[17]

This Article makes three novel contributions to AI ethics and privacy literature. First, this Article explains the prevalence of exploitation created through excessive data collection and use. Excessive exploitation results from an individual's significant exposure to continuous surveillance and compromised privacy within AI healthcare solutions.[18]

This Article explains normative expectations as expressed in U.S. privacy law in relation to the healthcare industry, one of the industries where excessive exploitation is most likely to occur and where such exploitation may be framed as justifiable within the public interest. Second, this Article illustrates how such exploitation of health data is perpetuated by AI technology development, including data collection and use that can justifiably improve fairness and safety. This challenge—that the very benefits for responsible AI can actually subject patients to exploitation—demonstrates the need for more inclusive analyses between often distinct scholarly fields.

Finally, this Article recommends a model for preventing excessive exploitation and explores how such a model could be implemented. This model builds on Frank Pasquale's and Jack Balkin's proposed information fiduciary,[19] narrowly applied to a subset of automated technologies in the health sector and the data they process.

This Article proceeds in four parts. Part I describes the contemporary nature of health technology and health data use that creates the scaffolding for excessive exploitation, including big data, advanced diagnostics, mobile health technologies, medical devices, and Internet of Health Things

[16] *See supra* notes 8, 9, 15.

[17] Individuals who may already be subject to discrimination may be further harmed by opaque algorithmic decision-making based on data that either (1) encodes historical discrimination or (2) nevertheless creates disparate impact. Sahar Takshi, *Unexpected Inequality: Disparate-Impact from Artificial Intelligence in Healthcare Decisions*, 34 J.L. & HEALTH 215, 223 (2021); Andrew Burt, *How to Fight Discrimination in AI*, HARV. BUS. REV. (Aug. 28, 2020), https://hbr.org/2020/08/how-to-fight-discrimination-in-ai.

[18] It is generally accepted that community norms are what create expectations of privacy and explain why there may be differentiation in reasonable expectations of privacy in Europe than in the United States, for example. James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1160–64 (2004) (describing differences between European countries and the United States, specifically distinct normative conceptions of harm, dignity, and liberty); ERIN KENNEALLY, USENIX ADVANCED COMPUTING SYS. ASS'N, REASONABLE EXPECTATIONS OF PRIVACY INDICATORS 2 (2016), https://www.usenix.org/system/files/conference/soups2016/wpi16_paper_kenneally.pdf.

[19] Frank Pasquale, *Toward a Fourth Law of Robotics: Preserving Attribution, Responsibility, and Explainability in an Algorithmic Society*, 78 OHIO ST. L.J. 1243 (2017).

("IoHT").[20] Part II describes how exploitation of individuals using healthcare technologies and the healthcare sector overall occurs, explaining the factors that increase the likelihood of excessive exploitation. Part III explores, in more detail, the foundations of trust and misplaced trust within the healthcare technology ecosystem, including how trust-based relationships can promote unethical behavior. Part IV proposes a framework for determining when an information fiduciary role may be appropriate in the healthcare sector. Part IV then further explores how the information fiduciary model can be implemented to avoid excessive exploitation.

I. CONTEMPORARY HEALTHCARE TECHNOLOGIES

AI is frequently depicted in the far-reaching future, but AI is being used today. From self-driving cars to advanced medical robotics, AI is used—often surreptitiously—by a wide variety of organizations and product manufacturers.[21] AI may take various forms, whether automating processes,[22] improving human decision-making,[23] improving safety and efficacy,[24] augmenting expertise,[25] or driving optimal machine functionality.[26] AI may

[20] Internet of Health Things are Internet-connected devices related to health management. For example, FitBits or connected weight scales might be considered IoHT but may not be considered regulated medical devices.

[21] Alex Engler, *The Case for AI Transparency Requirements*, BROOKINGS: AI GOVERNANCE (Jan. 22, 2020), https://www.brookings.edu/research/the-case-for-ai-transparency-requirements/.

[22] Naveen Joshi, *3 Key Differences Between AI and Robotics*, FORBES (Jan. 16, 2022, 7:30 AM), https://www.forbes.com/sites/naveenjoshi/2022/01/16/3-key-differences-between-ai-and-robotics/?sh=5bff0822d34d.

[23] Vinod Saratchandran, *6 Ways Artificial Intelligence is Driving Decision Making*, FINGENT (Sept. 9, 2019), https://www.fingent.com/blog/6-ways-artificial-intelligence-is-driving-decision-making/.

[24] Phil Britt, *How AI-Assisted Surgery is Improving Surgical Outcomes*, ROBOTICS BUS. REV. (June 19, 2018), https://www.roboticsbusinessreview.com/health-medical/ai-assisted-surgery-improves-patient-outcomes/.

[25] Steve Lasky, *AI is Leveraging Advanced Analytics for Physical Security Operations*, SECURITYINFOWATCH.COM (Jan. 14, 2022), https://www.securityinfowatch.com/access-identity/article/21253250/ai-is-leveraging-advanced-analytics-for-physical-security-operations.

[26] Riya Savjani, *5 Ways AI Can Optimize the Efficiency of Your Production Line*, EINFOCHIPS (July 3, 2020), https://www.einfochips.com/blog/5-ways-ai-can-optimize-the-efficiency-of-your-production-line/.

be embodied in robotics,[27] connected to sensors and other kinetics,[28] or it may be disembodied, as in software and mobile apps.[29]

Healthcare, a sector that stands to benefit from increased efficiency, improved quality, and reduced cost, is positioned to embrace AI and connected technologies as a means of providing more, better, and cheaper healthcare, a triad of goals usually not satisfied without sacrificing the others.[30] Health technology, in the form of big data, artificial intelligence, consumer wearables, and medical devices, *could* revolutionize the practice of medicine—if the U.S. can do so without permitting excessive exploitation of the very people who stand to benefit.

A. Big Data—Healthcare Providers, Insurers, Employers

The terminology "big data" is used heavily in a variety of sectors to describe exceptionally large data sets.[31] Big data may be used for purposes including advanced analytics, organizational operations optimization, and innovation. And yet, data are just information encoded in 0s and 1s in their most primitive form.

Despite this inauspicious form, data are powerful. Because data encode information about our world, our bodies, and ourselves, data are tremendously valuable, in aggregate and in relation to the individual to facilitate technology personalization.[32] Data matter because of what they can tell us about ourselves and how we interact with the world around us. Functionally speaking, data do not usually matter because of what they encode, but rather what they can tell us about the underlying systems that animate our lives.[33] Information is created simply by being, by living in a

[27] Nivash Jeevanandam, *The Ambitious Goal to Make Robots Act & Look More Real*, ANALYTICS INDIA MAG. (Oct. 1, 2021), https://analyticsindiamag.com/embodied-ai-nouvelle-ai/.

[28] Kaustubh Gandhi, *Sensors and Artificial Intelligence–A Powerful Symbiosis*, SENSOR SOLS. (Jan. 29, 2019), https://www.sensorsolutions.net/article/106270/Sensors_and_artificial_intelligence_-_a_powerful_symbiosis.

[29] Fraunhofer-Gesellschaft, *A Mobile App and AI Software to Speed Up Skin-Cancer Diagnoses*, MED. XPRESS (Feb. 1, 2022), https://medicalxpress.com/news/2022-02-mobile-app-ai-software-skin-cancer.html.

[30] WILLIAM L. KISSICK, MEDICINE'S DILEMMAS: INFINITE NEEDS VERSUS FINITE RESOURCES 2–3 (1994) (describing the "Iron Triangle" of cost, quality, and access); *How Artificial Intelligence Reduces the Cost of Doing Business*, QUYTECH (Dec. 16, 2019), https://www.quytech.com/blog/how-artificial-intelligence-reduces-the-cost-of-doing-business/.

[31] Nicolas P. Terry, *Big Data Proxies and Health Privacy Exceptionalism*, 24 HEALTH MATRIX 65, 77 (2014).

[32] Lizzie Ottenstein, *AI & Behavior: The Power of Personalization in Healthcare*, FUSEMACHINES (Dec. 4, 2020), https://insights.fusemachines.com/ai-behavior-the-power-of-personalization-in-healthcare/.

[33] W. Nicholson Price II & Arti K. Rai, *Clearing Opacity Through Machine Learning*, 106 IOWA L. REV. 775, 779, 809 (2021). Access to big data stores, especially those that are publicly

world, by making decisions. But data elements exist because someone or an organization chooses to document them.

Big data and its application in mobile technologies, advanced analytics, and artificial intelligence, have changed our lives because more and more information about our lives is being recorded—and, presumably, has value to someone.[34] Artificial intelligence and advanced analytics seek to tell us something about the world around us or our inner biological functions in a much more comprehensive fashion than ever before. These technological approaches maximize use of the machines that have always captured and recorded data, but in a way that does not superimpose human perceptions of how these underlying systems work.[35] Consider the following example:

> *Gelena has struggled with gastrointestinal issues throughout her life. As a young child, Gelena's father gave her glasses of milk to settle her stomach, which sometimes caused vomiting. After removing dairy from her diet, Gelena's symptoms improved. At age 10, Gelena began experiencing rectal bleeding, which a doctor determined was from a form of colitis. After completing a combined upper gastrointestinal endoscopy/colonoscopy, however, the doctor identified some intestinal inflammation, but not the type of inflammation usually associated with colitis or Crohn's disease. At age 14, Gelena began having problems eating wheat products and was diagnosed by another doctor with celiac disease. After removing wheat from her diet, Gelena managed not to have any serious medical issues until recently. Now 22 years old, Gelena has begun having nausea and serious stomach pain. Another doctor completed a full endoscopy/colonoscopy again and some blood tests, and she diagnosed Gelena with gastroparesis. Although Gelena is managing her gastroparesis by avoiding certain foods and taking pharmaceuticals to reduce the symptoms, there is no cure. At this time, Gelena is not able to maintain employment or care for her child due to the seriousness of her symptoms.*

The example above illustrates the type of situation where big data using AI diagnostic algorithms could be useful. In each one of the physician interactions described in the example, the physicians could only diagnose the

funded, is particularly desirable to promote transparency while buoying scientific discovery and reducing research costs. *See* Sharona Hoffman, *Citizen Science: The Law and Ethics of Public Access to Medical Big Data*, 30 BERKELEY TECH. L.J. 1741, 1755–56, 1761 (2015).

[34] *See generally* ADAM TANNER, OUR BODIES, OUR DATA: HOW COMPANIES MAKE BILLIONS SELLING OUR MEDICAL RECORDS (2017).

[35] Some AI systems are able to identify relationships between data elements more dynamically with little involvement by humans in classifying the data. *See* R. Sathya & Annamma Abraham, *Comparison of Supervised and Unsupervised Learning Algorithms for Pattern Classification*, 2 INT'L J. ADVANCED RSCH. A.I. 34, 35–37 (2013) (suggesting that unsupervised learning algorithms could be more effective in classifying individuals).

condition based on the information and tools available to them at the time, usually information provided by the patient and basic technological outputs. If data could be collected on an ongoing basis, in real-time, directly from Galena's body and using data Galena inputs into an app (what she ate and when, timing of digestive processes, and symptoms), perhaps doctors could better determine the cause of her health issues.[36]

However, more data alone does not equate to better results.[37] There is the real challenge of organizing data in such a way that it can be useful.[38] If data are collected from Galena's body via blood draws, gastrointestinal ("GI") imaging, barium X-rays, self-reported information, and a device like the PillCam™,[39] the raw data are likely to provide a more comprehensive view of Galena's potential diagnosis.

If these data outputs are then organized effectively, the probability of determining the root cause of Galena's illness increases, whether or not advanced AI technology is used, though AI technology is more likely to calculate relationships between data elements more effectively.[40] While the best GI experts in the world might be able to immediately determine Galena's problem from a multitude of data points, not all physicians have this expertise and not all patients like Galena have access to experts.[41] The solution may be creating health AI that can mine and analyze a significant volume of data from various health care providers and technologies. The resulting AI has been positioned as democratizing access to healthcare expertise, a real problem in healthcare deserts, such as under-resourced urban hospitals and rural healthcare systems.[42]

Imagine how much data might be collected through various tests, systems, and input by Galena in a mobile app. The probability of successfully

[36] Any one of these inputs could be useful for diagnostics, which is why patient self-monitoring on mobile device apps has become an important intermediary step for more effective diagnostics.

[37] Michael Grogan, *Why More Data Is Not Always Better*, MEDIUM (Aug. 8, 2020), https://towardsdatascience.com/why-more-data-is-not-always-better-de96723d1499.

[38] Marijn Janssen et al., *Data Governance: Organizing Data for Trustworthy Artificial Intelligence*, 37 GOV'T INFO. Q., July 2020, at 1, 2–3 (describing the need for data governance techniques to avoid poorly functioning AI technology).

[39] *PillCam™ SB 3 Capsule Endoscopy System*, MEDTRONIC (2022), https://www.medtronic.com/covidien/en-us/products/capsule-endoscopy/pillcam-sb-3-system.html.

[40] *See supra* note 35.

[41] W. Nicholson Price II, *Medical AI and Contextual Bias*, 33 HARV. J.L. & TECH. 65, 73 (2019).

[42] Charlotte A. Tschider, *Legal Opacity: Artificial Intelligence's Sticky Wicket*, 106 IOWA L. REV. ONLINE 126, 147 (2021) [hereinafter Tschider, *Legal Opacity*]. Limitations on data use and transfer subject to contracts may impede data collation for purposes like this. *Id.*; *see also* Price, *supra* note 41, at 90–99 (describing the risk of exporting expertise without considering the health context of such application).

mining the data to render an accurate diagnosis would likely increase substantially if computational resources could evaluate relationships within a large volume of structured data.[43] Based on data collected from patients like Galena, latent relationships between not only two data points but hundreds of thousands of patients with similar symptoms could improve diagnostic effectiveness. This is the type of function AI utilities can provide, with the potential to render (with sufficient data) a probabilistic determination such as "98% likelihood of Crohn's Disease" in less than a minute for an area of medicine that is notoriously difficult to accurately diagnose.[44]

Data and the infrastructure used to organize, mine, and analyze data are symbiotic: AI is rendered useless without adequately representative data.[45] And data without infrastructure are not useful, either: Without the machinery to mine and analyze them, statistical analysis will be ineffective, unfair, and even dangerous.[46] Combined big data sets, with different organizational provenances, are both highly desirable commercially and are necessary for effective health technology to operate, whether it is via mobile technologies, Internet of Health Things, or AI-enabled technologies.[47] To mobilize data sharing goals, organizations have created a legal mechanism, a data-sharing agreement, which explains in a detailed way what an organization may or may not do with data they receive.[48]

Medical devices using such data usually consist of five technological components: sensors, sensor fusion and algorithmic inferences, connectivity, infrastructure, and (for some medical devices) mobility and miniaturization.[49] It is the transition between the physical and the digital world that creates

[43] Lauren Maffeo, *AI's Next Breakthrough: Analyzing Unstructured Data in Healthcare*, GETAPP (Oct. 22, 2019), https://www.getapp.com/resources/unstructured-data-in-healthcare/.

[44] Ahmad El Hajjar & Jean-François Rey, *Artificial Intelligence in Gastrointestinal Endoscopy: General Overview*, 133 CHINESE MED. J. 326 (2020) (describing the use of AI in GI endoscopy).

[45] *See* Price, *supra* note 41, at 107–10; Price & Rai, *supra* note 33, at 792 (describing the difficulty of creating new data and needs for high volumes of data in AI); *supra* note 2; Charlotte A. Tschider, *Medical Device Artificial Intelligence: The New Tort Frontier*, 46 BYU L. REV. 1551 (2021) [hereinafter Tschider, *Medical Device Artificial Intelligence*].

[46] *See* Janssen et al., *supra* note 38, at 3.

[47] "Provenance" is used to determine from whom and where data originated. Data provenance is a concern for nearly all data implementations because once data are collected, they are often transferred to other parties without information about their origin attached. This causes significant issues for contract compliance and privacy laws that may prohibit data use under some circumstances.

[48] *See* Tschider, *Legal Opacity*, *supra* note 42, at 147.

[49] JOSHUA A.T. FAIRFIELD, OWNED: PROPERTY, PRIVACY, AND THE NEW DIGITAL SERFDOM 54–62 (2017).

privacy and security risks,[50] leading to the potential for physical injury, exploitation, or manipulation of individuals dependent on these devices.[51]

Many of these devices are not managed by the patient or even the healthcare organization through which the devices are used, and data produced by human-device collaboration are similarly not owned by the patient interfacing with the device.[52] Between medical device manufacturers and patients, exploitation is often framed as a legitimate exchange: to benefit from the technology, you must provide your data.[53] If a patient desires to manifest some choice over the situation, all a patient really has is a Hobson's choice: to use the AI technology and agree to extensive data collection or not use it at all. While this adhesive choice might be reasonably fair when purchasing a coffee maker, it is far from fair when presented with limited medical technology options to treat serious or fatal conditions pursuant to a doctor's recommendation.

B. Artificial Intelligence in Medical Technology

Artificial intelligence is used in a variety of medical applications. AI can increase operational efficiencies and decrease costs while improving care quality.[54] However, the most promising AI applications are those poised to

[50] *See generally* Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85 (2014) (describing potential issues with IoT devices and the data they collect).

[51] *See generally* Charlotte A. Tschider, *Regulating the Internet of Things: Discrimination, Privacy, and Cybersecurity in the Artificial Intelligence Age*, 96 DENV. L. REV. 87 (2018) [hereinafter Tschider, *Regulating IoT*] (describing the myriad of security, privacy, and potential physical issues introduced with IoT and AI combined); Charlotte A. Tschider, *Enhancing Cybersecurity for the Digital Health Marketplace*, 26 ANNALS HEALTH L. 1 (2017) [hereinafter Tschider, *Enhancing Cybersecurity*] (illustrating the cybersecurity concerns introduced by medical devices); Charlotte A. Tschider, Deus ex Machina*: Regulating Cybersecurity and Artificial Intelligence for Patients of the Future*, 5 SAVANNAH L. REV. 177 (2018) [hereinafter Tschider, Deus ex Machina] (describing the unique cybersecurity concerns for health AI specifically and their impact on the physical body); Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995 (2014) (illustrating the potential for manipulation through the digital marketplace).

[52] Niam Yaraghi & Joshua Bleiberg, *Your Medical Data: You Don't Own It, but You Can Have It*, BROOKINGS: TECHTANK (Apr. 28, 2015), https://www.brookings.edu/blog/techtank/2015/04/28/your-medical-data-you-dont-own-it-but-you-can-have-it/; *see* FAIRFIELD, supra note 49, at 2–3 (describing the simultaneous intrusion of devices into the most personal environments coupled with control over assets and data, a "digital serfdom"); Krista Kennedy, *Designing for Human-Machine Collaboration: Smart Hearing Aids as Wearable Technologies*, 5 COMMC'N DESIGN Q., no. 4, 2017, at 40, 40. Personal data is not personal property or intellectual property even though privacy obligations may apply to the handling of such data. Due to the non-status of data statutorily and under the common law, ownership in personal data is typically allocated via private ordering, as in a contract. *See* Jorge L. Contreras, John Rumbold & Barbara Pierscionek, *Patient Data Ownership*, 319 J. AM. MED. ASS'N 935, 935 (2018).

[53] *See* FAIRFIELD, *supra* note 49, at 89–90.

[54] *Accountable Care Organizations ACOs*, PERSIVIA (2022), https://persivia.com/accountable-care-organizations-acos/.

save lives or improve the quality of patients' lives. Four areas where AI may be especially useful are in medical diagnostics, AI robotics, implantable devices, and medical wearables.[55]

1. Medical Diagnostics: Arterial Imaging

One area of increased focus for AI is medical diagnostics. Although a variety of different medical diagnostics are seeing significant development and investment, medical imaging AI has received much attention in its ability to augment and improve the effectiveness and efficiency of radiological interpretation.[56] Arterys is one example of a successful company in AI radiological interpretation. Many AI products, however, are combining common medical procedures with diagnostics, such as lesion detection technologies used in colonoscopies.[57]

Arterys has created an AI platform that integrates with existing arterial imaging technologies, such as MRIs, CT scans, and X-rays.[58] To date, Arterys has developed platforms that focus on five major medical diagnostic areas: Breast, Cardio, Lung, Chest, and Neuro.[59] Importantly, Arterys claims to have implemented such a system and promoted data sharing while simultaneously protecting individual privacy,[60] which is a uniquely difficult feat in imaging generally.[61]

Arterys' approach has been to amplify physician effectiveness through "human + AI."[62] Arterys created 4D flow technology in an accessible, web-based format so that physicians can better visualize blood flow in arteries. Arterys' products consistently identify portions of the images that illustrate issues rather than relying on more subjective static image diagnostics.[63] In 2017, this technology received the first-ever U.S. Food & Drug Administration ("FDA") clearance for cloud computing and AI deep learning

[55] *See infra* Sections I.B.1–4.

[56] Seong K. Mun et al., *Artificial Intelligence for the Future Radiology Diagnostic Service*, FRONTIERS MOLECULAR BIOSCIS., Jan. 28, 2021, at 1.

[57] *FDA Authorizes Marketing of First Device that Uses Artificial Intelligence to Help Detect Potential Signs of Colon Cancer*, U.S. FOOD & DRUG ADMIN. (Apr. 9, 2021), https://www.fda.gov/news-events/press-announcements/fda-authorizes-marketing-first-device-uses-artificial-intelligence-help-detect-potential-signs-colon.

[58] ARTERYS, https://www.arterys.com/ (last visited Apr. 21, 2023).

[59] *Id.*

[60] *Id.* Arterys claims to share data "without sharing PHI."

[61] Eyal Lotan, Charlotte Tschider, Daniel K. Sodickson, Arthur L. Caplan, Mary Bruno, Ben Zhang & Yvonne W. Lui, *Medical Imaging and Privacy in the Era of Artificial Intelligence: Myth, Fallacy, and the Future*, 17 J. AM. COLL. RADIOLOGY 1159 (2020).

[62] *See* ARTERYS, *supra* note 58.

[63] *About Us*, ARTERYS, https://www.arterys.com/about-us (last visited Apr. 19, 2023).

in a clinical setting.[64] Arterys has also extended and enhanced its uses by encouraging AI developers to upload algorithms for specific applications.[65]

2. AI Surgical Robotics: The CyberKnife

Surgical robotics has transformed surgery as we know it, primarily by enabling minimally invasive surgical techniques for surgeries that require a greater degree of precision and control.[66] Minimally invasive surgeries using surgical robotics usually claim fewer complications, including lowered-risk of site infection, faster recovery, less pain, less blood loss, and smaller scars.[67] Surgical robots do not operate independently—they are designed to be used by a surgeon who has been trained to use the surgical robot. Surgical robots, however, use AI to determine surgical patterns and calculate appropriate angles and distances in submillimeters. They often work on a smaller plane than traditional surgeries, working in distances that cannot be gauged with the naked eye.[68]

The Computer Motion AESOP machine became the first FDA-approved robotic surgical medical device for endoscopic medical procedures in 1990.[69] But the most significant evolution in robotic surgery began in 2000 with the da Vinci Surgery System, which was approved for general laparoscopic surgery, and can be used for both adult and pediatric surgery.[70] The da Vinci introduced centimeter-thick arms and a three-dimensional visualization screen, enabling less contact with interior tissue, reducing the risk of infection. The "Endo-wrist" function precisely replicates the movement of surgeons themselves.[71] This physical housing has inspired the coupling of advanced kinetic movement and haptic sensors with artificial intelligence to

[64] *Id.* It should be noted that Arterys went through a 510(k) clearance process, which is a truncated review for low-risk AI, which may or may not accurately evaluate potential issues. *See* Tschider, *Medical Device Artificial Intelligence*, *supra* note 45, at 1607–08 (describing broad issues in tort recovery when devices have been reviewed by the FDA and the insufficiency of such a review).

[65] *For Developers, Clinical Researchers, and ML Scientists*, ARTERYS, https://www.arterys.com/developers (last visited Apr. 19, 2023). At the time of writing, Arterys had five commercialized algorithms, with forty-four non-Arterys algorithms on their website, some of which have been "FDA cleared," CE Mark (the EU FDA model for medical devices), or KFDA approved (the Korean FDA), while others are for research purposes only.

[66] *Robotic Surgery*, MAYO CLINIC (May 6, 2022), https://www.mayoclinic.org/tests-procedures/robotic-surgery/about/pac-20394974.

[67] *Id.*

[68] *Robotic Surgery: The Role of AI and Collaborative Robots*, ASS'N FOR ADVANCING AUTOMATION (July 9, 2019), https://www.automate.org/blogs/robotic-surgery-the-role-of-ai-and-collaborative-robots.

[69] David B. Samadi, *History and the Future of Robotic Surgery*, ROBOTIC ONCOLOGY, https://www.roboticoncology.com/history-of-robotic-surgery/ (last visited Mar. 2, 2023).

[70] *Id.*

[71] *Id.*

perform more effective surgical techniques and, in limited use cases, autonomous surgery.[72] The inclusion of AI in surgical robotics is highly variable, from some assistance to full automation.[73]

Artificial intelligence in surgical robotics enables two key functions: the preprogrammed goal and its ability to dynamically respond to the ever-changing surgical environment.[74] Preoperative planning is used prior to surgery and consists of using medical imaging AI and medical record data to determine how the surgical robot will be used.[75] Spatial landmarks and alignment between medical imaging sources determine the surgical field and feed into the surgical robot's preprogramming before surgery.[76] During surgery, AI converts the surgical field interior of a patient's body into a 3D rendering for physician visualization, differentiating tissue types, and estimating and executing surgical navigation.[77]

One example of AI-enabled surgery that combines advanced imaging and robotic treatment is the ACCURAY CyberKnife® S7™ System ("CyberKnife").[78] The CyberKnife delivers stereotactic radiosurgery ("SRS") and radiation therapy to treat various forms of cancer.[79] The CyberKnife is different from typical robotic surgery in that the CyberKnife can deliver non-surgical stereotactic treatments in submillimeter accuracy on numerous organs: the prostate, liver, brain, lung, spine, kidney, or pancreas.[80] The CyberKnife receives real-time imaging during radiation treatment, approaching tumors from thousands of angles to deliver radiotherapy to precisely the tissue that needs it.[81] CyberKnife AI reduces the effects on healthy tissue, improves post-surgical recovery, and reduces overall side effects.[82]

3. *Implantable Devices: Insulin Pumps*

Implantable devices, sometimes called implantable electronic medical devices ("IEMD"), increasingly use AI both to train devices for more

[72] Sandip Panesar et al., *Artificial Intelligence and the Future of Surgical Robotics*, 270 ANNALS SURGERY 223, 223 (2019).

[73] *Id.* at 223–24.

[74] *Id.*

[75] Xiao-Yun Zhou et al., *Application of Artificial Intelligence in Surgery*, 14 FRONTIERS MED. 417 (2020).

[76] *Id.* at 419.

[77] *Id.* at 419–20.

[78] ACCURAY, https://www.accuray.com/ (last visited Apr. 19, 2023).

[79] *Id.*

[80] *Id.*; *CyberKnife® S7™*, ACCURAY, https://www.accuray.com/cyberknife/ (last visited Apr. 19, 2023).

[81] *Id.*

[82] *Id.*

effective use and to routinely update their safety and efficacy based on new data supplied to the algorithms that inform device function and precision.[83] There are a wide variety of implantable devices currently on the market, such as brain stimulation devices, cochlear implants, nerve stimulators, and insulin pumps.[84] Prosthetic limbs controlled through a brain-machine interface ("BMI") have also received significant recent attention.[85]

One implantable or permanently affixed device beginning to use AI is the insulin pump, used to deliver insulin in an automated way.[86] Insulin pumps eliminate the need for direct insulin delivery using insulin syringes and are increasingly used for children, who benefit from continuous glucose monitoring and automated delivery.[87] Despite the invention of the insulin pump, individuals with Type 1 diabetes still struggle to achieve their glycemic goals, which has opened the door to AI-enabled insulin pump systems.[88]

The FDA granted DreaMed's Advisor Pro's ("Advisor Pro") de novo request in 2018.[89] The Advisor Pro is an AI-enabled decision-support tool. DreaMed's decisional support tool is fueled both by endocrinologist expertise and real-world use.[90] Data are collected both from the insulin pump itself and other devices, such as the self-monitoring of blood glucose and continuous glucose monitoring.[91] These data are then analyzed by the MD

[83] Alan Lai, *Part Human, Part Robot: The Future of Medical Implantables*, PURSUIT (Sept. 12, 2017), https://pursuit.unimelb.edu.au/articles/part-human-part-robot-the-future-of-medical-implantables.

[84] Shivani V. Tripathi & Eva A. Husrt, *Pacemakers, Deep Brain Stimulators, Cochlear Implants, and Nerve Stimulators: A Review of Common Devices Encountered in the Dermatologic Surgery Patient*, 45 DERMATOLOGIC SURGERY 1228, 1228 (2019); Ms. Smith, *Hacking Pacemakers, Insulin Pumps and Patients' Vital Signs in Real Time*, CSO (Aug. 12, 2018, 10:08 AM), https://www.csoonline.com/article/3296633/hacking-pacemakers-insulin-pumps-and-patients-vital-signs-in-real-time.html.

[85] *See supra* note 84.

[86] *What Are Insulin Pumps?*, WEBMD (Nov. 6, 2022), https://www.webmd.com/diabetes/insulin-pump.

[87] *See generally* Universität Leipzig, *Automated Insulin Delivery for Young Children with Diabetes via Android App: International Clinical Trial Shows Life-Changing Positive Effects for Children and Their Families*, SCIENCEDAILY (Jan. 26, 2022), http://www.sciencedaily.com/releases/2022/01/220126144158.htm (describing the evolution of insulin delivery from older children to younger children).

[88] Revital Nimri et al., *Insulin Dose Optimization Using an Automated Artificial Intelligence-Based Decision Support System in Youths with Type 1 Diabetes*, 26 NATURE MED. 1380, 1380 (2020).

[89] Amanda Pedersen, *How AI Is Personalizing Insulin Therapy for Diabetes Patients*, MED. DEVICE & DIAGNOSTIC INDUS. (June 18, 2018), https://www.mddionline.com/digital-health/how-ai-personalizing-insulin-therapy-diabetes-patients; *Device Classification Under Section 513(f)(2)(De Novo)*, U.S. FOOD & DRUG ADMIN. (May 1, 2023), https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfpmn/denovo.cfm?id=den170043.

[90] *Advisor Pro*, DREAMED DIABETES (Jan. 5, 2023), https://dreamed-diabetes.com/advisor/.

[91] *Id.*

Logic algorithm, which suggests optimization of basal rate, carbohydrate ratio (for diet), insulin sensitivity, and personalized diabetes management tips.[92]

4. Medical Wearables: Smart Hearing Aids

Smart hearing aids have hit the market, poised to revolutionize the social and economic lives of millions of Americans. Hearing aids are used by individuals of all ages in a variety of communities with different lifestyle needs. The hearing needs of an individual who is retired, active, and social are likely drastically different from a child in a school classroom and on the playground or a professor attending academic conferences. Often doctors refer a patient to an audiologist who can help to personalize settings and educate patients about the features of their aid.[93]

The Starkey Livio Edge AI ("Livio") is one example of such aids.[94] The Livio claims best-in-class listening through its AI-based learning system, "Edge Mode," that adjusts to your surroundings to provide the best listening experience possible.[95] The Livio also provides monitoring support for older adults. With the Livio, Starkey introduced integrated sensors, which can detect when an individual falls and may have seriously hurt themselves.[96] The alert system then sends an automatic message to designated people to notify them of the fall.

The Livio is compatible with the patient's mobile device, which integrates features of the Livio through the Thrive Hearing Control mobile app that also includes brain and body activity tracking, the Intelligent Assistant, and Mask Mode to enhance hearing when individuals are wearing masks.[97] The Intelligent Assistant provides voice recognition and Smart Assistance, similar to Alexa or Siri.[98] The Livio's "[e]asy personalized control" boasts the ability to adjust to an individual's unique lifestyle.[99] Ultimately, the Livio is designed to be worn continuously while seamlessly interfacing with not just the wearer's physical body but also with their lifestyle.[100]

[92] *Id.*

[93] *See* Kennedy et al., *supra* note 9.

[94] *Livio Edge AI*, STARKEY, https://www.starkey.com/hearing-aids/livio-edge-artificial-intelligence-hearing-aids (last visited Apr. 19, 2023).

[95] *Id.*

[96] *Id.*

[97] *Id.*; *Do More With the Thrive App*, STARKEY, https://www.starkey.com/hearing-aids/apps/thrive-hearing-control/overview#scroll-target (last visited Apr. 19, 2023).

[98] *See Livio Edge AI*, *supra* note 94.

[99] *See id.*

[100] *Id.*

These AI technologies demonstrate the potential for substantial medical improvements through technological advancement, including personalized treatment.[101] AI technology has the potential to improve the effectiveness of medical treatment,[102] from diagnosis to treatment for a point in time,[103] to pervasive medical condition management through engagement and adherence.[104] These technologies demonstrate not only the wide variety of medical products now available, but also the importance of data both in creating the algorithms that run these technologies and in optimizing their function over time.[105]

II. THE "NATURE" OF HEALTHCARE TECHNOLOGY DATA

Despite their relative point-in-time or continuous use, all medical device types described in Part I require data, including highly sensitive personal information, to (1) create the algorithms used,[106] (2) provide real-time adjustments for more effective device use,[107] and (3) provide personalized delivery of healthcare.[108] Machine learning algorithms cannot be created without data and depend on continuous data feeding to improve their effectiveness.[109] Data *essentialism* motivates ubiquitous data collection: Data are both necessary and at least partially identifiable due to the criticality of these devices to deliver tailored, personalized medicine.[110] Data essentialism, though, actually risks exploiting the very patients that the health care sector is designed to help: When data are absolutely required for medical devices to function safely and efficaciously, ubiquitous data collection can result under the guise of legitimacy.

[101] Thomas Davenport & Ravi Kalakota, *The Potential for Artificial Intelligence in Healthcare*, 6 FUTURE HEALTHCARE J. 94, 96 (2019).

[102] *Id.*

[103] *Id.*

[104] *Id.*

[105] *Id.* at 97.

[106] Even where algorithms may be selected as a starting point, training on a data set is necessary for the algorithm to evolve and become more effective. For this reason, data are used to test and tune and predefined models. Tom Taulli, *How to Create an AI (Artificial Intelligence) Model*, FORBES (July 11, 2020, 1:38 PM), https://www.forbes.com/sites/tomtaulli/2020/07/11/how-to-create-an-ai-artificial-intelligence-model/?sh=13ce03487a97.

[107] *What Is Artificial Intelligence in Medicine?* IBM, https://www.ibm.com/topics/artificial-intelligence-medicine (last visited Mar. 28, 2023).

[108] Alan Payne, *The Role of AI in Advancing Personalized Healthcare*, TECHRADAR (Sept. 22, 2020), https://www.techradar.com/news/the-role-of-ai-in-advancing-personalized-healthcare.

[109] Ben Lorica, *Why Continuous Learning Is Key to AI*, O'REILLY (Aug. 7, 2017), https://www.oreilly.com/radar/why-continuous-learning-is-key-to-ai/.

[110] *See* Tschider, *Legal Opacity*, *supra* note 42, at 153–54.

A. Personal Information in Medical Device AI

While the medical potential is great, data may exist solely because an organization surreptitiously collects, records, and uses data from a human being's passive and active technology use. Without a natural, biological human and the presence of a human body, these devices would not function to their potential, whether such data are collected during clinical trials or after clinical trials when the medical device is in commercialized use.[111]

"Human-machine collaboration," as coined by Dr. Krista Kennedy, elaborates this symbiotic relationship: As much as individuals need technology, technologies also need humans to provide data.[112] Despite the disembodiment of data once data are collected and stored on remote servers, these data exist in relation to the individual,[113] whether produced because of the human-computer interface or supplied from an independent source, such as medical records and medical imaging.

Medical devices using AI may be commercialized for broad use in locked or unlocked format. Locked algorithms are locked at the point of FDA submission and have been created based on the data humans have already supplied through their use in clinical trials.[114] Unlocked algorithms continuously adapt based on real-time device use.[115] Even when devices are used in "locked" format, the predominant type of AI the FDA has approved, human-device data is collected after commercialization to update the algorithms for a new release of the product.[116]

Overall, data collected continuously are the future of AI medical device development and could be transformative for device safety and efficacy.[117] Human medical device use might not cause much concern given its criticality for safety and effectiveness, but the nature of which data are used, how data

[111] *See* Tschider, *Medical Device Artificial Intelligence*, *supra* note 45.

[112] *See* Kennedy, *supra* note 52. At its base, human-machine collaboration necessarily requires some exchange of personal information for technical functionality, but it also involves a degree of dependency on the person to use the device and the device to help that person live. In this way, it is not transactional, as in consumer relationships, it is deliberately enmeshed.

[113] *See* Kennedy et al., *supra* note 9.

[114] MATTHEW DIAMOND, U.S. FOOD & DRUG ADMIN., PROPOSED REGULATORY FRAMEWORK FOR MODIFICATIONS TO ARTIFICIAL INTELLIGENCE/MACHINE LEARNING (AI/ML)-BASED SOFTWARE AS A MEDICAL DEVICE (SAMD): DISCUSSION PAPER AND REQUEST FOR FEEDBACK 3, 5 (2020), https://www.fda.gov/files/medical%20devices/published/US-FDA-Artificial-Intelligence-and-Machine-Learning-Discussion-Paper.pdf.

[115] *See* Tschider, *Medical Device Artificial Intelligence*, *supra* note 45, at 1572–73.

[116] *See* Tschider, *Legal Opacity*, *supra* note 42, at 133–35.

[117] Andrea Smith & Melissa Severn, *An Overview of Continuous Learning Artificial Intelligence-Enabled Medical Devices*, CANADIAN AGENCY FOR DRUGS & TECHS. IN HEALTH: HORIZON SCAN, https://canjhealthtechnol.ca/index.php/cjht/article/download/eh0102/704?inline=1 (last visited Mar. 28, 2023). Although continuous learning AI holds tremendous promise, without effective regulatory oversight, continuous learning AI could also present issues.

are used, and how algorithms actually make decisions (that will affect device functionality) are largely opaque as Frank Pasquale, Danielle Citron, Nicholson Price, and Arti Rai have explained.[118]

Organizations purposefully keep these practices confidential or secret, and technologically advanced algorithms may not be readable even by their creators.[119] The combination of both technical opacity and continuous changeability of such algorithms can be described as "dynamic inscrutability."[120] Dynamic inscrutability dramatically reduces the likelihood of effectively providing transparency of how decisions in AI are made.[121]

B. Health Data's Inherent Exceptionality

AI technology aside, the necessity of big data foundations for AI challenges traditional notions of the typical medical exchange: personal information supplied to receive medical services. In "small data" exchanges as in traditional medicine, the players are well-known and the formats and systems containing such data are reasonably expected.[122] For example, in small data implementations prior to passage of the Health Information Technology for Economic and Clinical Health Act ("HITECH") of 2009,[123] most health information was captured in paper health records.[124] The passage of HITECH, and later the 21st Century Cures Act,[125] served to modernize health transactions, including the portability of medical records between providers and submission of electronic insurance claims.[126]

Under the 1996 Health Insurance Portability and Accountability Act ("HIPAA")[127] and subsequent updates of the Privacy, Security, and Data

[118] *See* FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION 6–7 (2015); W. Nicholson Price II, *Black-Box Medicine*, 28 HARV. J.L. & TECH. 419, 433 (2015); Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 10 (2014); Price & Rai, *supra* note 33.

[119] Charlotte A. Tschider, *Beyond the "Black Box"*, 98 DENV. L. REV. 683, 688–91, 708 (2021) [hereinafter Tschider, *Beyond*].

[120] *Id.* at 705–06.

[121] *Id.*

[122] *See* Terry, *supra* note 31, at 66, 71.

[123] Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH), 42 U.S.C. § 17935 et seq.

[124] Leona Rajaee, *The History of Electronic Health Records (EHRs)*, ELATION: BLOGS (June 4, 2022), https://www.elationhealth.com/resources/blogs/the-history-of-electronic-health-records-ehrs-2.

[125] 21st Century Cures Act, Pub. L. No. 114-255, 130 Stat. 1033 (2016).

[126] Kushal T. Kadakia et al., *Modernizing Public Health Data Systems: Lessons from the Health Information Technology for Economic and Clinical Health (HITECH) Act*, 326 J. AM. MED. ASS'N 385 (2021).

[127] Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29, 42 U.S.C.).

Breach Notification Rules from 2001–2003 within that law, Congress (albeit indirectly) aimed to protect the privacy of individuals seeking services from healthcare providers and payment from health insurers.[128] The passage of HIPAA and later updates laid a path for protecting patient privacy while modernizing the healthcare experience for the benefit of patients and ease and efficiency for all parties involved.[129] When HIPAA was first enacted, Congress could not have anticipated the ways in which electronic data might be used by HIPAA regulated entities, including covered entities and their business associates, as well as subcontractors of business associates.

And yet, Congress did not pass a generally applicable privacy law as the European Union and several other countries in the European Economic Area had done just a year earlier in 1995.[130] Instead, Congress took the approach of passing sectoral laws, or laws that focused on sectors and populations where greater risks could exist: health, education, finance, electronic communications, and marketing activities.[131]

A significant motivation for passing these laws was the recognition that these sectors and data were sufficiently and inherently important, that data misuse could result in a variety of harms to individuals, and that a lack of compliance with specified practices demonstrates harm or risk of harm.[132] Such harm or risk of harm may be grounds for enforcement, including statutorily defined fines, *even if* the action itself does not result in data misuse or other generally recognized legal injuries, like financial impacts or job loss.

[128] The original goal of HIPAA was to ensure the portability of insurance from one job to the next, avoiding "job lock" where individuals would not change positions upon concern of losing insurance. The Privacy Rule was adopted in 2003, substantially later after two Administrations' worth of discussion on consent. *See* INST. OF MED., NAT'L ACAD. OF SCIS., BEYOND THE HIPAA PRIVACY RULE: ENHANCING PRIVACY, IMPROVING HEALTH THROUGH RESEARCH 1–2 (Sharyl J. Nass, Laura A. Levit & Lawrence O. Gostin eds., Nat'l Acad. Press 2009).

[129] However, the relatively narrow application of HIPAA has not created uniformity in health data obligations, focusing primarily on traditional healthcare players. In combination with state laws, considerable gaps remain. *See* Hoffman, *supra* note 33, at 1764.

[130] Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31 (EC).

[131] *See* Health Insurance Portability and Accountability Act of 1996 (HIPAA), 110 Stat. at 1936; Family Educational Rights and Privacy Act of 1974, Pub. L. No. 93-380, § 513, 88 Stat. 484, 571–74 (codified as amended at 20 U.S.C. § 1232g); Gramm-Leach-Bliley Act, Pub. L. No. 106-102, §§ 501–510, 113 Stat. 1338, 1436–45 (1999) (codified as amended at 15 U.S.C. §§ 6801–6809); Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, §§ 201–202, 100 Stat. 1848, 1860–68 (codified as amended at 18 U.S.C. §§ 2701–2710); Telephone Consumer Protection Act of 1991, Pub. L. No. 102-243, § 3, 105 Stat. 2394, 2395–2402 (codified as amended at 47 U.S.C. § 227); CAN-SPAM Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699 (codified as amended at 15 U.S.C. §§ 7701–7713).

[132] Privacy laws like HIPAA followed many of the recommendations of the U.S. Department of Health, Education and Welfare's study on statistical methods, including bifurcated consent. *See* Charlotte A. Tschider, *The Consent Myth: Improving Choice for Patients of the Future*, 96 WASH. U. L. REV. 1505, 1516–17, 1516 n.57 (2019) [hereinafter Tschider, *The Consent Myth*].

These laws had something important in common: The requirement of communicating a privacy notice (or privacy policy) specifying planned uses, actually restricting data use to disclosed uses and, in the case of HIPAA, a general requirement of data minimization.[133] It is important to consider why notifying individuals about data collection and requiring minimal collection and use of data was included in HIPAA at all.

If Congress really cared about data misuse, for example, they might have only passed requirements to notify patients of misuse and levied fines for such misuse. If Congress had simply wanted to reduce the probability of data breaches and subsequent sale of health data, Congress would not have had to pass the Privacy Rule at all, focusing instead on security and data breach notification, such as HIPAA's Security and Data Breach notification rules.[134] Considering the various rules and requirements collectively established under HIPAA, this suggests that Congress was trying to do something more: perhaps bolster individual choice and autonomy.[135]

HIPAA has contemplated data loss and data misuse as injuries in and of themselves by requiring organizations to notify affected individuals, the Department of Health and Human Services ("HHS"), and the media for larger data breaches.[136] HIPAA also statutorily permits the Office for Civil Rights ("OCR"), the enforcement arm of the HHS, discretion in enforcing non-compliance with HIPAA.[137] Although HIPAA does not provide for a right of private action, the existence of the OCR and its enforcement directive illustrates that Congress believed that misuse of data, even misrepresentation of privacy practices in a privacy notice, posed some risk to patient autonomy and choice regarding highly personal information.[138]

[133] 45 C.F.R. §§ 164.502(b), 164.514(d) (2023).

[134] *Id.* §§ 164.302–164.318; *id.* §§ 164.400–164.414.

[135] It should be noted that mechanisms for bolstering individual autonomy perhaps would have been sufficient in 1973 when these mechanisms were initially discussed. Since that time, data volume and potential uses have exploded, creating new ubiquitous computing processes that have rendered many of these mechanisms ineffective. *See generally* Tschider, *The Consent Myth*, *supra* note 132 (describing the "consent myth," or the issues, or problems, related to relying on notice and consent in a healthcare context and compromising autonomy).

[136] 45 C.F.R. §§ 164.404, 164.408, 164.406 (2023). In the case of a business associate, a third party of a primary covered entity under HIPAA, the business associate must notify the covered entity. *Id.* § 164.410.

[137] *Id.* §§ 160.306, 160.308, 160.312, 160.314, 160.400–160.426, 160.500–160.548.

[138] Enforcement actions illustrate this as well. Enforcement actions frequently describe a failure to provide privacy notices or adequately obtain authorization for data use. For example, recent enforcement actions have focused on the failure to fulfill a patient's right of access to their medical records, a right that has more to do with information and choice than with potential risk of data loss or fraud. *See Five Enforcement Actions Hold Healthcare Providers Accountable for HIPAA Right of Access*, U.S. DEP'T OF HEALTH & HUM. SERVS. (Jan. 23, 2023), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/2021-right-of-access-initiative/index.html.

It is this desire to promote autonomy and choice that is a central function of privacy law overall, not just preventing tangible harms and legally-defined injury.[139] This distinction is important—creating models that bolster autonomy through strong privacy practices is consistent with existing privacy laws. Because harms to autonomy may not be recoverable and concrete injury in litigation, it is essential that statutory regimes intercede with appropriate administrative enforcement.[140]

Although the United States has not established privacy as a civil right like most countries in the European Economic Area, the importance of choice (via consent) at the outset of such laws laid the foundation for considering that collecting personal information carries some inherent risk of abuse.[141] This inherent risk in privacy may be considered deontological, or a risk in and of itself absent some secondary tangible harm, or consequentialist risk.[142]

An example of an inherent, deontological risk of harm to individual privacy is overcollection. For example, overcollection of data beyond what is needed for the technology to function does not, on its own, lead to a privacy violation or data breach that compromises a person's financial interests. Although it may be difficult to label the uncomfortable feeling of loss when data are collected and then used beyond the bounds of reasonableness, an individual's autonomy is degraded to some extent.

[139] *See infra* Part III.

[140] Article III requirements for standing limit injury claims to those that demonstrate an injury in fact when such injury is fairly traceable to the defendant's conduct, and it is likely to be redressed by the court. Lujan v. Defs. of Wildlife, 504 U.S. 555, 560–61 (1992). Such injury must be concrete and particularized to the individual bringing the action. *Id.* at 560 n.1. In 2016, the United States Supreme Court determined that although the United States Court of Appeals for the Ninth Circuit may have properly evaluated particularized injury in *Spokeo, Inc. v. Robins*, 578 U.S. 330 (2016), a case where an individual brought a statutory-based cause of action based on individual statutory rights that had been infringed, the Ninth Circuit did not adequately analyze whether the injury was sufficiently concrete: actual or imminent, not conjectural or hypothetical. *Id.* at 339–40, 342. Congress may not erase the Article III requirements by granting a right to sue where there is no standing. *Id.* at 342. Concreteness means that an injury must actually exist. *Id.* However, concreteness may be satisfied by risk of real harm. *Id.* at 341–42 (referencing the holding of *Clapper v. Amnesty International USA*, 538 U.S. 398 (2013)). Procedural violations of a statute, for example, may be enough to demonstrate injury. *Id.* Although the law may be evolving for privacy injury and the *Spokeo* holding may have been positioned as promising for cases involving less tangible injury, the reality is that the Court has not provided a wide berth for injuries to an individual's autonomy, injuries that are inherently intangible and may not demonstrate risk of "real harm" as defined by courts.

[141] It could be argued that not all personal information carries these potential harms, and furthermore, it seems that the *practices* by an organization in a position of power were similarly concerning. Taken together, Congress seems to be concerned about certain practices in relation to statutorily defined sensitive personal information, combined risks of power, exploitation, and injury.

[142] *See* Price & Cohen, *supra* note 8.

C. Big Health Data's Exceptional[143] *Characteristics*

Big data implementations, necessary to create all AI products, have dramatically changed the nature and degree of privacy risks. "Small data" are the data collected in limited volumes but essential for the function of certain AI, for example data present in medical records, such as a specific pharmaceutical prescription or an illness and medical visit date, data that existed before medical data digitization.[144] Contemporary health data is both highly sensitive and collected and stored in significant volumes.[145] Today's "big data" in healthcare use a myriad of data sources, including feeds from Electronic Health Record ("EHR") systems, device outputs, public data, and patient inputs.[146]

Big data include much more than the small data of yore: Big data include device data specific to the individual's treatment or device use, as well as proxies[147] for sensitive data gleaned through big data inferences and supplemental data, such as the Livio's capture of environmental location data or music playlist choices. These data sets may also include cellular location data—data which may be indirectly indicative of health conditions.[148] The primary difference between big data and small data in healthcare is the size and the degree of inferences, inferences that may nevertheless be able to identify a sensitive characteristic.[149]

Increasingly, and if used correctly, to the benefit of the individual, healthcare is concerned with risk factors that affect a person's health, such as socioeconomic status, race and generational trauma, genetic history, and a

[143] Nicolas Terry describes healthcare privacy law as exceptionalism, in that the data protected and organizations regulated under healthcare privacy law are notoriously narrow. *See* Terry, *supra* note 31, at 66. The narrow application of these laws with significant attendant obligations both prior to collection and for later use leaves out a wealth of health data collected and used outside the traditional health privacy regulatory structure. *See* Joel Gurin & Paul Kuhne, *Report: Why Health Data Privacy Needs More than HIPAA*, FEDSCOOP (Sept. 24, 2019), https://www.fedscoop.com/report-health-data-privacy-needs-hipaa/.

[144] For example, big data are created by machines, but small data are principally about the person. *See* H. James Wilson & Paul R. Daugherty, *Small Data Can Play a Big Role in AI*, HARV. BUS. REV. (Feb. 17, 2020), https://hbr.org/2020/02/small-data-can-play-a-big-role-in-ai; Alexandra Chang, *Small Data and Big Health Benefits*, CORN. UNIV. RSCH. & INNOVATION, https://research.cornell.edu/news-features/small-data-and-big-health-benefits (last visited Apr. 19, 2023).

[145] Not only is the privacy regulatory structure exceptional; health data itself may present many of the same characteristics.

[146] Privacy and security issues have long been concerns for EHR systems given their large footprint and potential for privacy violations and data breaches. *See* Sharona Hoffman & Andy Podgurski, *E-Health Hazards: Provider Liability and Electronic Health Record Systems*, 24 BERKELEY TECH. L.J. 1523, 1555–57 (2009).

[147] *See* Terry, *supra* note 31, at 66, 87.

[148] Anya E.R. Prince, *Location as Health*, 21 HOUS. J. HEALTH L. & POL'Y 43, 52–56 (2021).

[149] *See* Terry, *supra* note 31, at 87, 97.

myriad of other community characteristics.[150] Healthcare data, like location data, has the unique ability to signal other sensitive characteristics, especially when broad data, in furtherance of more comprehensive healthcare, is analyzed using advanced artificial intelligence.[151]

For example, dietary data collected in a mobile app for an AdvisorPro insulin pump may be designed to supplement calculations of optimal insulin dosage. However, such data collected over time could suggest, with a high degree of reliability, an individual's religious practices. Data on eating habits might otherwise seem innocuous and may appear to be non-identifiable, yet data from restaurants or regional staples might nevertheless pinpoint an individual's home location, nationality, work location, or ethnicity. Location data could similarly identify an individual's health condition, such as frequent trips near a dialysis clinic.[152]

Health data, as captured through a combination of small data coupled with additional data, can be identifiable, even if steps have been taken to remove sensitive data elements, such as a medical device serial number, healthcare visit date, full name, or date of birth.[153] What's more is that personal data are *created* by using the device. In the case of Arterys or CyberKnife, the data collected during a diagnostic activity or treatment

[150] David R. Williams et al., *Race, Socioeconomic Status, and Health: Complexities, Ongoing Challenges, and Research Opportunities*, 1186 ANNALS N.Y. ACAD. SCIS. 173, 174–76 (2010); Michelle M. Sotero, *A Conceptual Model of Historical Trauma: Implications for Public Health Practice and Research*, 1 J. HEALTH DISPARITIES RSCH. & PRAC. 93, 94–95 (2006); Niha Zubair et al., *Genetic Predisposition Impacts Clinical Changes in a Lifestyle Coaching Program*, SCI. REPS., May 2, 2019, at 1, 8 (finding that genetic predisposition can affect the success of a lifestyle coaching program involving human wellness and disease management); INST. OF MED., NAT'L ACADS. OF SCIS., GENES, BEHAVIOR, AND THE SOCIAL ENVIRONMENT: MOVING BEYOND THE NATURE/NURTURE DEBATE 25 (Lyla M. Hernandez & Dan G. Blazer eds., 2006), http://nap.nationalacademies.org/11693. Furthermore, genetic data presents unique challenges for protection, including the high degree of identifiability alongside an inability to adequately de-identify such data. *See* Hoffman, *supra* note 33, at 1771–72. Therefore, it is likely that such data used within AI applications will introduce a high risk of identification that cannot be neutralized by de-identification.

[151] *See, e.g.*, Rachel Gordon, *Artificial Intelligence Predicts Patients' Race from Their Medical Images*, MIT NEWS (May 20, 2022), https://news.mit.edu/2022/artificial-intelligence-predicts-patients-race-from-medical-images-0520 (describing how AI could predict race from medical images alone, undetectable by doctors); Anil Aswani & Yoshimi Fukuoka, Opinion, *Artificial Intelligence Could Identify You and Your Health History from Your Step Tracker*, USA TODAY (Jan. 28, 2019, 5:00 AM), https://www.usatoday.com/story/opinion/2019/01/28/health-privacy-laws-artificial-intelligence-hipaa-needs-update-column/2695386002/ (describing how more sensitive health data can be derived from comparatively less sensitive consumer behavior monitoring).

[152] *See* Prince, *supra* note 148.

[153] Liangyuan Na et al., *Feasibility of Reidentifying Individuals in Large National Physical Activity Data Sets from Which Protected Health Information Has Been Removed with Use of Machine Learning*, J. AM. MED. ASS'N NETWORK OPEN, Dec. 21, 2018, at 1. Using machine learning, re-identification of de-identified data is possible. *Id.* at 2. This study demonstrates that even for high-variability data, such as physical activity data, re-identification is still possible with sufficiently powerful AI systems. *Id.* at 7–10.

procedure is necessarily specific to an individual's unique bodily characteristics, such as the shape or condition of tissues or organs.

While these data elements may not be individually sensitive data points from the perspective of identity theft, such as an electronic health record number, these data are extensions of the physical body and inherently individual, as unique as a fingerprint or a retinal scan, and similarly sensitive.[154] Although such data may not independently indicate biological gender or race, often such data are captured in combination with such procedures.[155]

Health data are exceptional not only in their big data form but because of their essential relationship to the human body and relative permanence. Unlike a credit card number that can be changed, data collected through medical records, imaging scans, and medical device use digitally approximate who (at least in part), biologically, physically, and potentially mentally, a person is. Medical devices that technically connect or integrate with external devices, such as mobile devices, frequently include lifestyle and location data that expand this pool significantly.

When data are replicated and shared, even when they are not sensitive, they are data created by a person's interface with technology and derived from that relationship. Furthermore, AI medical device use is *designed* to be personal and, in some cases, enmeshed: The very reason why AI medical devices are desirable is that they can adapt and learn from an individual's unique characteristics.[156] Without personal bodily data created through human-computer analog and non-AI digital devices, such devices would not work as effectively.[157]

D. Data Identifiability Risk Mitigation Techniques

If an organization collects a large volume of sensitive data and seeks to promote patient interests, organizations might consider making these data

[154] For example, biospecimen information and genetic data are both considered personally identifying data. *See Coded Private Information or Specimen Use in Research, Guidance (2008)*, U.S. DEP'T OF HEALTH & HUM. SERVS. (June 4, 2019), https://www.hhs.gov/ohrp/regulations-and-policy/guidance/research-involving-coded-private-information/index.html (defining private information and specimens when they can be linked to individuals by principal investigators directly or indirectly).

[155] Romana Hasnain-Wynia & David W. Baker, *Obtaining Data on Patient Race, Ethnicity, and Primary Language in Health Care Organizations: Current Challenges and Proposed Solutions*, 41 HEALTH SERVS. RSCH. 1501, 1502 (2006). Capturing this data is essential for identifying differences in care that may be problematic and for delivering specific interventions based on population groups.

[156] *See* Tschider, *Beyond*, *supra* note 119, at 707.

[157] *See* Tschider, *Legal Opacity*, *supra* note 42, at 130.

less identifiable, through pseudonymization or de-identification.[158] It makes intuitive sense: When it is difficult or improbable that an individual can be identified, there is less overall risk of harm to that individual. However, big data frustrates most accepted de-identification techniques in the United States, and the risks of exploitative harm are far more multi-faceted than simply whether data are de-identified or not.

HHS's De-Identification Safe Harbor ("Safe Harbor"), for example, permits organizations regulated under HIPAA to legally use data without restriction, so long as it has been de-identified.[159] The general notion is that de-identified data pose very little risk to a specific patient, which theoretically means that using data to satisfy an organization's interests is not legally or ethically problematic.[160] These uses could include data that can create new technologies or to improve upon old ones, transferring to partners or affiliates, or selling de-identified big data sets for commercial profit.

Why might an organization do this? Because health data, even de-identified data, are highly desirable for other organizations to expand their big data repositories.[161] For example, insurers may request medical device data to understand device use and efficacy for reimbursement purposes. Other organizations developing new medical products may also benefit from access to these data. When AI systems are trained and running, data are not optional: they require large, organized data volumes to develop safe, effective, and fair algorithms.

1. De-identification and Anonymization of Big Data

There are two models for de-identifying data under the HIPAA Safe Harbor defined by the Department of Health and Human Services: either the removal of eighteen common identifiers or expert determination.[162] These

[158] SIMSON L. GARFINKEL, NAT'L INST. OF STANDARDS & TECH. NISITR 8053, DE-IDENTIFICATION OF PERSONAL INFORMATION 15–26 (2015), http://dx.doi.org/10.6028/NIST.IR.8053.

[159] *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. (Oct. 25, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html [hereinafter HHS, *Guidance*]. Of course, the narrow application of the Safe Harbor to HIPAA covered entities and their business associates leaves many data custodians managing health data simply unregulated. *See* Hoffman, *supra* note 33, at 1768–70.

[160] *See* GARFINKEL, *supra* note 158, at iii.

[161] Claire Biot et al., *Data Sharing Is Key to Innovation in Health Care*, MIT TECH. REV. (Sept. 27, 2019), https://www.technologyreview.com/2019/09/27/132847/data-sharing-is-key-to-innovation-in-health-care/; *Patient Data Is a Hot Commodity. Here's How Third Parties (Legitimately) Get Ahold of It.*, ADVISORY BD. (Apr. 10, 2018), https://www.advisory.com/daily-briefing/2018/04/10/patient-data.

[162] *See* HHS, *Guidance*, *supra* note 159.

eighteen identifiers are largely indicative of a small data world, including identifiers that are common in provisioning healthcare, such as date of birth or date of visit.[163] Expert determination requires a third party to apply statistical methods to certify a data set as de-identified and "low risk" to the patient.[164] The de-identification model, however, does not necessarily address the increased risk of identifiability within big data sets related to the scale and volume of additional data.[165]

In contrast, requirements of anonymization, as is the case under EU law, requires an "impossibility of reidentification" standard rather than a low risk of re-identification, requiring a higher standard of protection.[166] For example, current U.S. law permits pseudonymization, where an organization may maintain fully identifiable data sets for disclosed uses, but separate identifiable sets from non-identifiable data to create two databases.[167] The database containing "non-identifiable" data according to the Safe Harbor can be shared, used without restriction, or sold.[168] The EU would prohibit this behavior, as well as increase the threshold for demonstrating a data set can be shared with nearly no risk to the patient.[169]

2. Big Data Identifiability & AI Personalization

De-identification, pseudonymization, and anonymization may appear to be panaceas for all the potential risk of harm patients could face.

[163] *Id.*

[164] *Id.*

[165] Mowafa S. Househ et al., *Big Data, Big Problems: A Healthcare Perspective*, 238 STUD. HEALTH TECH. & INFORMATICS 36, 38 (2017); *see* Hoffman, *supra* note 33, at 1769–70. Notably, the Safe Harbor permits pseudonymized data sets, wherein identifiable data are temporarily segregated from de-identified data but designed to be re-identified when a functional data set is needed. These data sets, temporarily segregated, count as de-identified, even when security applied to such data sets would not actually enforce their segregation. Ultimately, what this means is that data sets could be readily identified by those seeking to do harm to patients or use their data for nefarious purposes, such as insurance fraud. *See* HHS, *Guidance*, *supra* note 159.

[166] *Anonymization*, EUR. COMM'N: COLLABORATION IN RSCH. & METHODOLOGY FOR OFF. STAT. PORTAL, https://ec.europa.eu/eurostat/cros/content/anonymization_en (last visited Apr. 20, 2023) (citing Regulation 2016/979 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and of the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119)).

[167] *See* HHS, *Guidance, supra* note 159.

[168] Raj Sharma, *The Privacy Myth of De-Identified Medical Data*, MEDIUM: HEALTH WIZZ (Oct. 1, 2017), https://medium.com/healthwizz/the-privacy-myth-of-de-identified-medical-data-10b9678e4bea; Nichole Wetsman, *Hospitals are Selling Treasure Troves of Medical Data – What Could Go Wrong?*, VERGE (June 23, 2021, 2:22 PM), https://www.theverge.com/2021/6/23/22547397/medical-records-health-data-hospitals-research.

[169] *Opinion of the Article 29 Data Protection Working Party on Anonymisation Techniques* 0829/14/EN WP 216 (Apr. 10, 2014), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

Unfortunately, when organizations use more stringent data identity reduction techniques, data become less useful.[170] Due to their sheer volume and inferential power, big data sets also pose a greater risk of identification.[171]

For example, de-identified data in enough volume can illustrate patterns that ultimately tell us something personal about the individual or even re-identify the individual, without using pseudonymization at all.[172] These inferences may be innocuous or justifiably applied if an organization uses them to advance the interests of patients. The difficulty is in knowing whether greater collection and use of such personal information benefits the patient and public health, or whether it primarily benefits organizations.

Realistically, although the Safe Harbor may not adequately protect patients in a big data world, anonymized data probably are not as useful for AI medical device innovation and ongoing functionality.[173] Although privacy-preserving (or enhancing) technologies can improve individual privacy, there is an inevitable loss in data fidelity.[174] Indeed, the lack of available useful data could impede important health technology developments.[175] Some organizations typically use and maintain full data sets, at least for some period of time; other organizations may create pseudonymized data sets. This means that although risk to patients may be reduced, full, highly identifiable data are located somewhere.[176]

Collection and use of large identifiable data volumes may be required for safety, efficacy, or fairness in some contexts and may be excessively exploitative in others. AI medical devices require big health data for safety and efficacy, big data produced through the human-computer interface, rendering data that are highly valuable and necessary to current and ongoing

[170] Laetitia Kameni & Laura Degioanni, *Can We Solve the Data Privacy/Utility Problem?*, ACCENTURE (Feb. 4, 2022), https://www.accenture.com/us-en/blogs/technology-innovation/kameni-degioanni-can-we-solve-the-data-privacy-utility-problem.

[171] For example, such inferences could be supplemented by AI explanations combined with data. *See* Tschider, *Legal Opacity*, *supra* note 42, at 152.

[172] *See* W. Nicholson Price II, *Problematic Interactions Between AI and Health Privacy*, 2021 UTAH L. REV. 925, 926–27; Kathleen Benitez & Bradley Malin, *Evaluating Re-Identification Risks with Respect to the HIPAA Privacy Rule*, 17 J. AM. MED. INFORMATICS ASS'N 169, 177 (2010) (explaining techniques for measuring re-identification risk); Latanya Sweeney et al., *Re-Identification Risks in HIPAA Safe Harbor Data: A Study of Data from One Environmental Health Study*, TECH. SCI. (Aug. 28, 2017), https://techscience.org/a/2017082801/ (describing a substantial risk of re-identification in one example of HIPAA de-identification Safe Harbor data).

[173] Lea Kissner, *Deidentification Versus Anonymization*, INT'L ASS'N OF PRIV. PROS. (June 18, 2019), https://iapp.org/news/a/de-identification-vs-anonymization/.

[174] André Calero Valdez & Martina Ziefle, *The Users' Perspective on the Privacy-Utility Trade-Offs in Health Recommender Systems*, 121 INT'L J. HUM. COMPUT. STUD. 108, 110 (2019).

[175] *See* Price & Rai, *supra* note 33, at 793–94.

[176] *Best Practices and Techniques for Pseudonymization*, ISC^2 BLOG (June 14, 2021), https://blog.isc2.org/isc2_blog/2021/06/best-practices-and-techniques-for-pseudonymization.html.

AI functionality.[177] Although HIPAA and its subsequent updates have laid the groundwork for identifying the unique and inherently risky nature of health data collection, use, and retention, it has not kept pace with contemporary big data and AI practices.[178]

Health data, especially health data used in AI and inferences created by AI, may pose substantial privacy risk to an individual.[179] Datafication, or separating the human from data, risks data overuse and may ignore data provenance.[180] Datafication as distinct from digitization takes "all aspects of life" and renders them as data,[181] removing the human and making it far more likely that organizations will engage in excessive exploitation. Big data are not simply big data due to their size; the advantage of big data is that it can "render into data many aspects of the world that have never been quantified before."[182]

When patients provide data about themselves and such data are combined with other patient data and external data sources, datafication is even more likely, as the human source of such data extend further and further away from the originally collected data set. It becomes easy for data scientists and other organizational decision-makers to use data for whichever purposes they choose, especially because recombining data often loses any original data provenance. As a result, largely for-profit companies make decisions about data use without considering the humanity of their data sources. And due to inherent asymmetries in knowledge about how collected data will actually be used or with which data the collected data will be combined, patients have very little awareness and choice over data about themselves.[183]

III. PRIVACY RISK AS EXPLOITATION

The key to understanding whether given practices are demonstrably legitimate or excessively exploitative is necessarily contextual and

[177] *See* Tschider, *Beyond*, *supra* note 119, at 692–94.

[178] *See* Price, *supra* note 172, at 931–32; Tschider, *Enhancing Cybersecurity*, *supra* note 51 (describing the limits of HIPAA in protecting health devices from cyberattack threats); Charlotte A. Tschider, *AI's Legitimate Interest: Towards a Public Benefit Privacy Model*, 21 HOUS. J. HEALTH L. & POL'Y 125 (2021) [hereinafter Tschider, *AI's Legitimate Interest*] (describing the ineffectiveness of notice and consent for advanced healthcare technologies).

[179] *See* Price, *supra* note 172, at 928.

[180] Minna Ruckenstein & Natasha Dow Schüll, *The Datafication of Health*, 46 ANN. REV. ANTHROPOLOGY 261, 264–65 (2017).

[181] Kenneth Cukier & Viktor Mayer-Schoenberger, *The Rise of Big Data: How It's Changing the Way We Think About the World*, 92 FOREIGN AFFS. 28, 35 (2013).

[182] *Id.* at 29.

[183] *Id.* at 37–38.

nuanced.[184] There are no bright-line rules like the Safe Harbor to facilitate such an investigation. Determining whether data collection and use is exploitative of individuals likely depends on how much data is actually necessary for devices to be fair, safe, and effective; or whether exploitation is so excessive that organizations dehumanize patients reliant on these devices.

As explained in Parts I and II, advanced healthcare technologies are positioned to transform human health, yet these technologies require substantial data. Substantial data collection may power these technologies and make them more effective, but these data may be highly identifiable, as collected, collated, or inferred. Moreover, the datafication of the individual may result in organizations making decisions that are not in the best interests of patients.

A. Harms that Create Excessive Exploitation

To understand how an individual may be exploited, it is important to first understand how exploitation can occur. Capitalistic exploitation is central to capitalism, the social frame for information collection and use in the AI medical device business community.[185] But regardless of this social frame, exploitation often is indicated by asymmetrical exchanges, and its relative, expropriation, occurs from direct confiscation of resources.[186] Although it is possible that data and money exchanged for products or services *may* be symmetrically exchanged, it is far more likely that both the exchange and the underlying power relationships are coercive, whether due to information asymmetries or power differentials.[187]

To rebalance personal information asymmetries that can cause harm to patients, it is essential to determine what harms and what circumstances demonstrate excessively exploitative practices. Despite the law's orientation towards consequentialist harms, privacy laws like HIPAA seem to suggest compliance obligations that can be construed as deontological and consequentialist.[188]

[184] *See* Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793, 812–13 (2022).

[185] MARIANO ZUKERFELD, KNOWLEDGE IN THE AGE OF DIGITAL CAPITALISM: AN INTRODUCTION TO COGNITIVE MATERIALISM 115, 122 (Suzanna Wylie trans., 2017).

[186] *Id.* at 122.

[187] *See infra* note 197.

[188] *See* Price & Cohen, *supra* note 8.

1. Understanding Exploitation as Harm

Although the term "exploitation" may be used colloquially as a value-neutral expression of using something to one's advantage,[189] exploitation also has several meanings within specific types of law, including elder law, criminal law, and race and the law. Exploitation usually means "to take unfair advantage" of someone or "to use another person's vulnerability for one's own benefit."[190] The biggest challenge is determining when exploitation exceeds our community norms of acceptability, that is when such exploitation is not *mutually* advantageous, or when such advantages are grossly disproportionately benefitting one party.[191] Excessive exploitation may be positioned as a form of unfairness, in that exploitation creates advantages for an entity (or individual) A at some cost to an individual B.[192]

Exploitation may be transactional or structural—unfairness may be based on discrete relationships or endemic to the entire system.[193] Moreover, what is initially exploitative but normatively acceptable may become excessive as society changes. Exploitation may be excessive at a particular scale or when an organization or individual uses a person or a data approximation of that person for unacceptable reasons, or harmful exploitation.[194] Exploitation may be analyzed from the perspective of an individual or in the aggregate, depending on how the harm occurs.[195]

The reasonableness of an organization's or individual's behavior is analyzed in relation to individuals who may be exploited; the question of exploitation is necessarily relational, not only what an organization (or individual) is doing, analyzed as if it is in a vacuum. We can only identify a "wrong" with respect to these relationships. For example, personal information may be collected, sold, and then used for independent commercial gain with no corresponding benefit to an individual or the

[189] Alan Wertheimer, *Exploitation in Health Care*, *in* PRINCIPLES OF HEALTH CARE ETHICS 247, 248 (Richard E. Ashcroft et al. eds., 2d ed. 2007).

[190] Matt Zwolinski & Alan Wertheimer, *Exploitation*, STAN. ENCYCLOPEDIA OF PHIL. (Aug. 16, 2016), https://plato.stanford.edu/archives/fall2016/entries/exploitation/.

[191] *See* Wertheimer, *supra* note 189, at 249–50.

[192] *Id.*

[193] *See* Zwolinski & Wertheimer, *supra* note 190; Matt Zwolinski, *Structural Exploitation*, 29 SOC. PHIL. & POL'Y, 154, 154–56 (2012) (describing how exploitation can be mutually beneficial, even when there is serious injustice lurking in the background political and economic institutions against which such decisions are made).

[194] *See* Wertheimer, *supra* note 189, at 249. Benefits to both parties need not be equivalent to be fair, but the process for divvying up such benefits must be. *Id.* at 251.

[195] *See* Zwolinski, *supra* note 193, at 170 n.55; *see also* Citron & Solove, *supra* note 184, at 816.

legitimate interests of the individual.[196] But exploitation also results from the extensive and often pervasive collective exposure of patients to commercial surveillance, often within disproportionate relationships of power that leave individuals with few choices. As Mark Andrejevic explains:

> For both legal and regulatory purposes, the notion of privacy, narrowly construed, is insufficient for the task of thinking about the pressing issues surrounding information collection and use. Like labour power in the industrial era, personal privacy is something that individuals surrender in exchange for access to resources – and they do so under structured power relations that render the notion of free or autonomous consent at best problematic.[197]

A primary issue related to data collection and use is whether consent can be free or autonomous. Assuming a party has the capacity and legal ability to consent, exploitation may not (on its face) seem problematic. So-called *consensual* exploitation can exist when such consent is "sufficiently voluntary, informed and competent."[198] However, despite the use of consent in healthcare transactions involving personal information, exploitation may not be consensual at all.

It may not be that easy to shed exploitative practices, despite the veneer of well-meaning objectives. Government entities and insurers might be motivated by a desire to collect data about underrepresented communities to improve coverage or services,[199] such as from people of color, people who have immigrated to the United States, or individuals with disabilities or rare health conditions.[200] Data must be high quality and representative to be

[196] *See generally* Tschider, *AI's Legitimate Interest*, *supra* note 178. (recommending an alternative to notice and consent that requires organizations to demonstrate that their data processing is in the individual's legitimate interest).

[197] Mark Andrejevic, *Privacy, Exploitation, and the Digital Enclosure*, 1 AMSTERDAM L.F. 47, 48 (2009).

[198] *See* Wertheimer, *supra* note 189, at 250.

[199] *See Data & Benchmarks*, CTRS. FOR DISEASE CONTROL & PREVENTION (Nov. 22, 2022), https://www.cdc.gov/publichealthgateway/cha/data.html (describing efforts to use community health assessments to produce primary and secondary data); Jessica Kim Cohen, *Who's Being Insured?*, MOD. HEALTHCARE (Sept. 6, 2022, 5:00 AM), https://www.modernhealthcare.com/insurance/insurers-taking-multipronged-approach-race-ethnicity-data-collection (describing insurers' approach to community health data collection); Sharona Hoffman, *Medical Big Data and Big Data Quality Problems*, 21 CONN. INS. L.J. 289, 295 (2014); *Data Veracity: A New Key to Big Data*, MEDIUM: SCIFORCE (July 11, 2019), https://medium.com/sciforce/data-veracity-a-new-key-to-big-data-38e110391c7d.

[200] *See* U.S. DEP'T HEALTH & HUM. SERVS., OFF. OF THE ASSISTANT SEC'Y FOR PLAN. & EVAL., IMPLEMENTATION GUIDANCE ON DATA COLLECTION STANDARDS FOR RACE, ETHNICITY, SEX, PRIMARY LANGUAGE, AND DISABILITY STATUS (2011), https://aspe.hhs.gov/sites/default/files/private/pdf/76331/index.pdf. The COVID-19 pandemic similarly identified key issues in data collection for these communities, as well. *See, e.g.*, *REALD*

useful,[201] and non-representative data may actually be dangerous. Government and insurer data collection objectives may be critically important to social goals, such as correcting longstanding health disparities in these communities and to benefit individuals who live at the intersection of multiple communities that require special consideration.

"Consensual" exploitation frequently occurs in relationships where the individual has little choice except to reject services altogether and where such services are necessary to an individual's life or quality of life.[202] For example, individuals who need emergency surgery may not be able to retain any legal rights over biological samples collected during the surgery.[203] Yet, it is unlikely for an individual to reject emergency surgery over such a requirement due to the exigency of the situation. Given a choice after the surgery has concluded, the patient may change their mind. Such situations will likely occur related to data when an individual is reliant on government assistance, when receiving employer-provided insurance, or when the technology is medically necessary or optimal for health management. Forced functional trust in an entity may be necessary to facilitate these activities, regardless of an individual's actual trust for an entity.

Exploitation is inherently relational—an individual cannot be exploited without an exploiter. Unsurprisingly, then, exploitation often occurs within and alongside relationships of trust (whether legitimate or forced) as manipulation.[204] Sometimes even "prosocial" deception can create trust,[205] though such trust arguably harms individual autonomy. It is a natural concern of trust-based relationships that they may be leveraged to exploit a less powerful or knowledgeable person,[206] which is precisely why the law enforces duties of care and loyalty for statutorily defined professionals.[207]

Data Collection and Reporting, OR. HEALTH AUTH., https://www.oregon.gov/omb/Topics-of-Interest/Pages/REALD-Data-Reporting.aspx (last visited May 4, 2023).

[201] Hoffman, *supra* note 199, at 295–98 (describing the fallacy that simply because we have "big" data does not mean that it is quality data). Although Hoffman focuses to some degree on the insurance industry, the problem of quality, representative, and curated data is an issue for safety and fairness, too. *See supra* note 119 (describing potential issues, both from a technology and data perspective, for safety and fairness).

[202] Such consent under these situations is generally consensual when it is not coerced. *See* Wertheimer, *supra* note 189, at 250. However, several critics of consent to information collection and use practices have demonstrated why such consent is almost always coerced.

[203] Carlo Petrini, *Ethical and Legal Considerations Regarding the Ownership and Commercial Use of Human Biological Materials and Their Derivatives*, 3 J. BLOOD MED. 87, 89 (2012).

[204] *See* Wertheimer, *supra* note 189, at 251. Presumptively, some trust must exist for manipulation to be successful.

[205] Jeremy A. Yip & Maurice E. Schweitzer, *Trust Promotes Unethical Behavior: Excessive Trust, Opportunistic Exploitation, and Strategic Exploitation*, 6 CURRENT OP. PSYCH. 216, 217 (2015).

[206] *Id.* at 216.

[207] *Fiduciary Duty*, BLACK'S LAW DICTIONARY (11th ed. 2019).

Not all exploitation is harmful: Some exploitation can be mutually beneficial, leaving both parties better off, though exploitation frequently and disproportionately benefits the more powerful party.[208] Exploitation is usually harmful, at least in part, to one party while being beneficial to the other. Although exploitative practices are common in surveillance capitalism generally, excessive exploitation may result when commercial benefits exceed patient benefits.[209]

2. Deontological and Consequential Harms

A deontological harm is framed as a harm in and of itself, a harm to the dignitary interests of the individual.[210] For deontological harms, the risk of harm is inherent in an act or failure to act, so the harm occurs when the action or failure to act occurs.[211] For example, a deontological harm would result from using personal information without authorization for undisclosed purposes, distributing personal information to a third party without the patient's knowledge, or collecting excessive personal information for the disclosed purposes.[212] The most important of human values, including freedom, democracy, civility, community, and creativity are all bolstered by

[208] *See* Yip & Schweitzer, *supra* note 205, at 216. As Yip & Schweitzer observe "trust has been defined as the willingness to be vulnerable to exploitation based upon positive expectations." *Id.*

[209] Exploitation is typically framed as connected to commercial activities, as in labor generation, and was largely criticized by Karl Marx. Although it could be argued that simply using a medical device or producing data through living is not "labor," data have substantial commercial value, especially for AI medical devices. *See* TANNER, *supra* note 34, at 15–16 (describing the medical industry cases where substantial income is made). Indeed, exploitation is central to free market, capitalistic models. In a capitalistic society, such exploitation is just part of the equation. Although perfect elasticity would hypothetically establish an optimal price for health technologies, healthcare is famously inelastic, and the data accompanying such transactions are not accounted for in price. Åke Blomqvist, *Optimal Non-Linear Health Insurance*, 16 J. HEALTH ECON. 303, 303–04 (1997). Therefore, if exploitation is tied at least in part to value exchanged, it may actually be a central feature of the healthcare industry requiring special consideration. SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM 43 (2019). Zuboff cites historical modernization of people with a reversion to premodern society: "what is unbearable is that economic and social inequalities have reverted to the preindustrial 'feudal' pattern but that we, the people, have not." *Id.* Zuboff continues to explain that "surveillance is a foundational mechanism in the transformation of investment into profit . . . commandeer[ing] the wonders of the digital world to meet our needs for effective life, promising the magic of unlimited information and a thousand ways to anticipate our needs." *Id.* at 52.

[210] Jim A.C. Everett et al., *The Costs of Being Consequentialist: Social Inference from Instrumental Harm and Impartial Beneficence*, 79 J. EXPERIMENTAL SOC. PSYCH. 200, 200 (2018); Price & Cohen, *supra* note 8, at 38.

[211] Everett et al., *supra* note 210, at 200–01; Price & Cohen, *supra* note 8, at 38.

[212] Deontological harms can also extend to forms of manipulation as well as circumstances where individuals are treated as a means to an end. *See* Ido Kilovaty, *Legally Cognizable Manipulation*, 34 BERKELEY TECH. L.J. 449, 470 (2019).

privacy.[213] These values are deontological because they bring about the development of human autonomy.[214]

Consequentialist theories define "moral rightness exclusively in terms of what produces the best consequences."[215] In this model, only consequences of an act are considered, not the act in and of itself. Therefore, consequentialist harm refers to downstream, concrete harms set into motion, consequences of the action or failure to act.[216] For example, consequentialist harm could be a failure to implement security measures, resulting in a data breach that causes identity theft.

The nature of data loss and misuse does not easily fit within this very limiting perspective, and associated harms could look very different than the Court may expect.[217] Privacy laws in the United States, including HIPAA, gesture to both deontological and consequentialist harms, though concrete consequentialist harm is typically how courts identify compensable harm in the form of legally cognizable injury.[218] Most privacy harms are illustrated as consequential, such as increasing the probability of identity theft.

Data overcollection would be a deontological harm to the individual's autonomy.[219] If describing deontological harm, we might instead explain that an organization harms an individual by exploiting them more than their non-exploited peers with no additional benefit.

Without a more expansive acknowledgement that both types of harms "count" for privacy law, we fail to understand how individuals can be negatively harmed through their exploitation. Understanding harm more expansively to include both deontological and consequential harms is necessary for understanding excessively exploitative practices.[220]

[213] *See* Citron & Solove, *supra* note 184, at 818.

[214] Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1428 (2000).

[215] Jonathan Quong, *Consequentialism, Deontology, and Distributive Justice*, *in* OXFORD HANDBOOK OF DISTRIBUTIVE JUSTICE 308 (Serena Olsaretti ed., 2018).

[216] *Id.*

[217] Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 740 (2018). As Solove and Citron explain, the Court in *Clapper v. Amnesty International USA*, 568 U.S. 398 (2013), reiterated that standing requires "injury that is concrete, particularized, and actual or imminent (as opposed to hypothetically possible)." Solove & Citron, *supra*, at 740 (citing *Clapper*, 568 U.S. at 409). Indeed, the plaintiffs could not show proof that injury was imminent. *Id.* The Court continued to explain that in some instances, "substantial risk" that the harm will occur is sufficient. *Id.* at 741 n.14 (quoting Susan B. Anthony List v. Driehaus, 573 U.S. 149, 158 (2014)).

[218] *See* Citron & Solove, *supra* note 184, at 826–27. Even for consequential harms, such harms must illustrate a degree of certainty in their occurrence (i.e., non-speculative).

[219] When courts have even begun to explore deontological and less concrete types of privacy harms, the focus is on collection *and* use. *Id.* at 827.

[220] There are countless examples of regulating the risk of harm in administrative law generally, and specifically in privacy law. For example, data breach notification laws may include legal

It might be easy to write off deontological privacy harms in this context as non-exploitative because data are part of the healthcare transaction. After all, a patient needs the DreaMed pump or will benefit from a less invasive surgery using the Cyberknife. If a patient needs the pump, or will benefit from Cyberknife surgery, why should organizations not be able to collect data from them in trade for access to these innovative technologies? This presumptive transactive framing of the problem is not helpful: After all, the medical device and the surgery will be compensated through actual payment; these entities are not *paid* in personal information and health data. Data are ancillary to the transaction but may be essential to some effective functionality of the technology. This is part of the reason why questions of information are often outside the present exchange of product or service and frequently subject to statutory obligations rather than common law recovery.

B. Risk and Statutory Obligations to Avoid and Transcend Risk

Much of privacy law deals in the language of risk (of harm), and privacy statutes are designed to reduce risk to the individual person. Medical device regulation similarly seeks to reduce risk from a safety, rather than a privacy, risk perspective. Neither of these statutory landscapes demand perfection. The expectation is one of *reasonableness* and good-faith effort.[221] Compliance functions within organizations similarly note non-compliance or partial compliance with a statutory requirement as "risk," or risk of harm, whether such harm is deontological or consequential.[222]

1. Defining Risk of Harm

In privacy law, consequentialist risks of harm are focused on consequences: The harm may be actual monetary losses, job loss, or denial of entitlements or other services that results from a data breach, data misuse, or discrimination. Deontological risks are tied to inherent, dignitary, or moral

requirements, but many only require that organizations notify an individual if their unencrypted personal information has been subject to a data breach. *See, e.g.*, 45 C.F.R. §§ 164.400–164.414 (2023) (data breach notification requirements under HIPAA). Notification requirements are designed to promote self-protection on the part of the affected individual to reduce the degree of harm.

[221] For tort, such practices must be reasonably foreseeable, and such foreseeability is either construed based on reasonable duties that are expected to be owed to another party or, as under negligence per se, when published statutorily providing a private right of action.

[222] *See* Quong, *supra* note 215; Sven Ove Hansson, *Risk*, STAN. ENCYCLOPEDIA OF PHIL. (Dec. 8, 2022), https://plato.stanford.edu/entries/risk/.

harms, such as overcollection or overuse of personal information. For this reason, they are sometimes called duty or obligation-based ethics.[223]

Under statutory regimes, risks are mitigated by a combination of proscriptive actions an organization must take to prevent harm, such as describing practices an organization uses with respect to personal information, and an individual's opportunity to agree to practices that might otherwise be excessive. This agreement, usually described as "consent," legally neutralizes any perceived exploitative practices by documenting the individual's consent to such practices. Privacy laws include preventative requirements, such as conducting risk assessments, displaying a privacy notice, or requiring an accounting of data uses.

Preventative requirements illustrate a model consistent with deontological risks: By mandating organizations restrict how much data are collected to only what is strictly necessary to fulfill business purposes or limit data collection to disclosed purposes in a privacy notice, no consequentialist harm results from failing to do this. However, intrinsically having your data used without knowing what is used and for what purposes (for example, selling someone's personal information for profit without their knowledge) simply *feels* wrong. This illustrates that although consequentialist risks certainly matter, privacy law has historically recognized some degree of deontological risk for individual people. Statutes may also include responsive requirements, such as data breach notifications, reporting safety issues, performing data access requests, or corrective actions that reduce the potential for consequential harms.

2. Overcoming Risk of Harm through Private Ordering

Organizations may seek to overcome any risk of harm by enabling the person or patient to consent to information handling practices. For example, additional processing of personal data in a healthcare context is not prohibited. Rather, organizations simply need to execute the appropriate paperwork: For healthcare operations, confirmation of the Notice of Privacy Practices receipt, and for additional data processing, an authorization form, is statutorily required.[224] This model is framed as "fair," promoting individual choice, and, therefore, promoting autonomy. The challenge, however, is that notice and consent, procedures positioned to overcome any risks associated

[223] David Misselbrook, *Duty, Kant, and Deontology*, 63 BRIT. J. GEN. PRAC., Apr. 2013, at 211, 211, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3609464/pdf/bjgp-april2013-63-609-211.pdf.

[224] Tschider, *The Constent Myth*, *supra* note 132, at 1513–15.

with excessive data collection and use, do not actually eliminate deontological or consequentialist risks of harm.[225]

As Daniel Solove, Neil Richards, Woodrow Hartzog, and this author have explained, consent is an imperfect substitute for meaningful choice, at least if the law values individual autonomy.[226] Helen Nissenbaum has described the importance of autonomy in relational and contextual constructs, reminding us that autonomy can inform choice when these choices are "guided by principles . . . adopted as a result of critical reflection."[227]

The effectiveness of consent as choice is determined by the degree by which human autonomy is diminished in the process. Consent simply cannot overcome deontological risk of harm because human patients are in a lesser position of power and information with respect to the healthcare ecosystem. Such dynamics make human choice largely uninformed and usually involuntary, depending on the context in which it is used.[228]

3. Private Ordering through Statute

Private quasi-contracts in the form of a Privacy Notice are usually required under privacy laws. Public drafters of privacy legislation seem to expect notice and consent to overcome bad practices—affected individuals have the power to refuse detrimental practices after reviewing the privacy notice and seek other products or services.[229] However, privacy notices coupled with consent do not cure imprecise and non-salient language that apprises an individual of actual risk, and the sheer number of privacy notices presented to individuals makes it nearly impossible to read all of them anyway.[230] Privacy notices have largely evolved to be exercises that protect the organization from liability rather than actually inform individuals of risk to them.[231]

[225] The concept of consent as a complete defense to any number of torts is well-known. Charlotte A. Tschider, *Meaningful Choice: A History of Consent and Alternatives to the Consent Myth*, 22 N.C. J.L. & TECH. 617, 627–28 (2021) [hereinafter Tschider, *Meaningful Choice*].

[226] *See* Tschider, *AI's Legitimate Interest*, *supra* note 178, at 165–68. *See generally* Tschider, *The Consent Myth*, *supra* note 132 (describing the consent myths that render consent ineffective in a healthcare context); Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880 (2013) (describing how consent is largely ineffective, but paternalistic models present additional issues); Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461 (2019) (describing how contemporary models for consent are largely ineffective).

[227] Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 148 (2004).

[228] *See* Richards & Hartzog, *supra* note 226, at 1492.

[229] *Id.* at 1474–75.

[230] M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027, 1065–67 (2012); *see* Tschider, *The Consent Myth*, *supra* note 132, at 1520–26 (describing voluntariness, structural, cognition, exogeneity, and temporal problems).

[231] *See* Richards & Hartzog, *supra* note 226, at 1471.

Privacy laws like HIPAA do require additional protective steps, such as adhering to the Security Rule, notifying patients of data breaches and unauthorized use, and permitting patients to revoke consent in addition to other data subject rights.[232] However, these protections are largely procedural (and sometimes performative) because they can be executed without much consideration of the person at all, sometimes involving extensive data uses without explaining corresponding benefit or risks to the individual. Procedural requirements do not correct pre-existing exploitative dynamics in health technology: power, trust, and opacity. Although privacy laws are written to address deontological and consequentialist harms, they do not consider these exploitative dynamics.

Despite Congress's *desire* to motivate individual autonomy through choice, current privacy models build on rotten scaffolding—adhesive and usually patently unfair scaffolding that ignores substantial power dynamics and commercial interests that lead to exploitation. These dynamics are always present for consumers generally but are significantly more problematic and exploitative in healthcare due to (1) the exceptional nature of healthcare data (as described in Parts I and II), (2) the power dynamics and existing fiduciary relationships present in healthcare relationships and specifically for AI technologies, and (3) the opaque nature of AI medical products.

C. Relational Trust and "False Trust"

As scholars such as Neil Richards, Woodrow Hartzog, and Ari Waldman have explained in great detail, trust is essential in any relationship, including relationships between organizations and individuals.[233] Richards and Hartzog, for example, have noted that trust-based relationships may prove useful in defining how information relationships *could* work and evolving the nature of these relationships based on reasonable expectations of loyalty.[234] Ari Waldman has described privacy as a social norm of information based on trust.[235] A relational conception of privacy is needed to better understand our commitments to each other, relationships that consider

[232] 42 C.F.R. § 403.812; *id.* §§ 164.400–164.414; *id.* § 164.508(b)(5).

[233] Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431, 447 (2016) [hereinafter Richards & Hartzog, *Taking Trust Seriously*]; Neil Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 WASH. U. L. REV. 961 (2021) [hereinafter Richards & Hartzog, *Duty of Loyalty*]. *See generally* ARI EZRA WALDMAN, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE (2018).

[234] *See* Richards & Hartzog, *Taking Trust Seriously*, *supra* note 233, at 457.

[235] *See* WALDMAN, *supra* note 233, at 67.

"what powerful parties owe to vulnerable parties."[236] Without real and legitimate trust-based relationships, real privacy is also unattainable.

1. Trust Intermediaries

Improving relationships between humans and organizations developing medical AI technologies is a challenge, as largely human-to-human relationships of trust have been replaced by human-computer interfaces.[237] Today's "trust" in healthcare technology is often created through one-way communication from an organization to an individual with quasi-contractual notices and acting in accordance with those notices. There is typically no meaningful opportunity for feedback on communicated practices, except with a doctor that, even if they are involved with the healthcare process, probably does not understand how data are collected and used.

More contemporary notions of trust in these relationships include providing individuals with the ability to act on their own interests via design factors that permit an individual to granularly make decisions about their information, such as discrete and modular privacy preferences.[238] However, the common issues that plague all consumer privacy notices similarly affect patients, such as voluntariness (coercive consent), structural issues (privacy policy fatigue), cognition (understanding such privacy notices), exogeneity (unawareness to internal and complex technology practices), and temporal problems (the inability for a technology company using AI to specifically describe how data will be used prior to it being collected).[239]

2. False Trust

Although enhancing trust should be a central goal of all privacy relationships, it is precisely the existence of a trust-based relationship in healthcare AI technology that complicates goals of greater trust. The special relationship between doctor and patient has existed for a lengthy period of time and has been enshrined in fiduciary obligations because the doctor is in a position of trust and relative expertise. False trust may appear to be genuine when pre-existing fiduciary relationships, despite a doctor not having relative expertise, when individuals apply this trust to how their data might be collected and used.

[236] Neil Richards & Woodrow Hartzog, *A Relational Turn for Data Protection?*, 4 EUR. DATA PROT. L. REV. 492, 493 (2020).

[237] *See* Tschider, *The Consent Myth*, *supra* note 132, at 1512. The replacement of individual trust relationships, where discussions might be conducted in-person with a human being, with form privacy notices, has not buoyed crucial relationships of trust. *Id.*

[238] WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES 63–64 (2018).

[239] *See* Tschider, *The Consent Myth*, *supra* note 132, at 1519–26.

The doctor-patient relationship is the sacrosanct foundation of healthcare: It is how data are gathered, how diagnoses and plans are formed, how patients are supported, and, where possible, how healing occurs.[240] If a patient does not have a trust-based relationship with their doctor, information will not be disclosed efficiently or at all, potentially harming their health outcomes.[241] The most vulnerable of patients must trust their doctors.[242] Trust may be essential to privacy, but privacy is essential to trust, too.[243] Because doctors cannot know or control all of the ways in which data are collected, used, stored, shared, or transferred when they rely on third parties, traditional ways of facilitating trust through knowledge, openness, and honesty are much more difficult to achieve.[244]

False trust for health technology takes advantage of the essential nature of a high degree of trust in traditional healthcare relationships. The following illustrate how false trust can develop:

(1) A preexisting fiduciary relationship, such as the doctor-patient relationship, cannot effectively perform its function (e.g., advising on potential risks and benefits related to data);

(2) Transference of the expectations of a fiduciary relationship to the manufacturer-patient relationship, a non-fiduciary relationship; and

(3) A lack of available information due to legal and technical opacity that could otherwise enhance trust.

As described by Jeremy Yip and Maurice Schweitzer, individuals are more likely to be exploited within relationships of trust.[245] Trust is a natural consequence of asymmetric relationships of power, knowledge, or expertise when the individual needs or depends on the other party. Individual consumers or patients must trust parties with more knowledge, information, or expertise. Certain demographics are more trusting and, therefore, more likely to be exploited, such as older adults who may be dependent on certain health devices, such as monitoring technologies, that keep them at home.[246]

[240] Susan Dorr Goold & Mack Lipkin, Jr., *The Doctor–Patient Relationship: Challenges, Opportunities, and Strategies*, 14 J. GEN. INTERNAL MED. S26, S26 (1999).

[241] *Id.*

[242] *Id.* at S27. Indeed, "[t]rust is most realistic when a relationship has a history of reliability, advocacy, beneficence, and good will." *Id.* at S29 (citing an unnamed, unpublished manuscript by R.L. Jackson).

[243] *Id.* at S32. As Goold and Lipkin rightly mentioned in their 1999 article, "confidentiality is no longer solely in the doctor's control." *Id.*

[244] *Id.* at S31–S32.

[245] *See* Yip & Schweitzer, *supra* note 205, at 217.

[246] *Id.* at 217–18.

3. Fiduciary Relationships

The existence of a fiduciary relationship in healthcare complicates trust surrounding the use of AI medical devices. Under the law, usually under statute or contract (and occasionally under court determination), medical fiduciary relationships are established. The law narrowly defines fiduciary relationships to enumerated persons and situations where a special relationship of trust exists, though the term "fiduciary" does not actually define who a fiduciary must be.[247]

Statutes and courts define fiduciaries in this way because fiduciaries are expected to perform their duties on an ongoing basis, sometimes even after the relationship has ended.[248] The goal in a fiduciary relationship is to prevent harms from occurring—harms that result from fiduciaries acting in their own interest rather than the individual's—which principally involve a duty of loyalty and, in the case of physicians, a duty of care.[249] A fiduciary "exercises discretionary power over the significant practical interests of another."[250]

The goal of narrowly defining such relationships is two-fold: to put individuals on notice when their position of power, and of trust, will result in reliance on them, and second, to determine when additional duties may be expected of them. When a fiduciary does not perform their duty, it is usually viewed by society not just as a legal failing, but often a moral one, too. For example, a doctor's recommendation for a patient to use a medication for a purpose not indicated on the label resulting in serious harm will likely be viewed differently than a manufacturer recommending the same thing.[251] Despite this isolated distinction, in a complex treatment relationship, this distinction may not be apparent.

Although patients may advocate for their health or even conduct their own research, doctors still stand in a position of expertise—and hold themselves out as such. Broadly requiring an average person to perform the

[247] PAUL B. MILLER, *The Fiduciary Relationship*, *in* PHILOSOPHICAL FOUNDATIONS OF FIDUCIARY LAW 64–66 (Andrew S. Gold & Paul B. Miller eds., 2014).

[248] One exception does apply in tort law but only when injury occurs: the undertaker's duty. The undertaker's duty applies when an individual takes some positive action for another in such a way that prevents or dissuades others from taking that action. Classically, the duty is applied when a person is in obvious need of aid. For example, if a restaurant patron is choking and someone walks toward them to give help, it is expected that the other person will, in fact, try to help them. If they do not, the person could have received help from someone else.

[249] Defining a fiduciary relationship is less crucial than defining what is expected when such relationships apply. *See* MILLER *supra* note 247, at 66 & n.12 (quoting P.D. Finn, *The Fiduciary Principle in Equity*, *in* EQUITY, FIDUCIARIES, AND TRUSTS 26 (T.G. Youdan ed., 1989)).

[250] *Id.* at 69.

[251] The concepts of medical malpractice and products liability are two distinct areas of tort law for a reason, usually because the existence of a fiduciary relationship changes the nature of the duties and the harm.

exact same duties as medical professionals probably does not make sense[252]: We expect individuals to look out for their best interests generally, rather than believe anyone they might encounter.

Fiduciary relationships also exist because there is inherently greater risk associated with the activities between a fiduciary and an individual, in particular when the beneficiary relies on the fiduciary's knowledge to choose or advise a course of action.[253] For example, the same doctor recommending a patient take an experimental drug for which they are receiving financial incentives may be breaching their duty of loyalty, resulting in the patient being injured (a treatment paid for by the patient, their insurer, or the government). When a fiduciary gets it wrong, there are far greater impacts for the individual.

Moreover, fiduciary relationships exist because we, as a society, *want* people to trust fiduciaries in a relationship.[254] Trusting fiduciaries and being a fiduciary worth trusting is good for society and for the economy when patients trust their doctors, customers trust their banks, and clients trust their attorneys. The presence of fiduciary relationships gives everyone greater confidence in the system, greasing the wheels of any number of commercial relationships and information disclosures.[255] And, perhaps optimistically, society also cares about individual autonomy. Individuals should be able to make informed decisions in their best interests, relying on experts to help them.

4. Fiduciaries, Pseudo-Fiduciaries, and False Trust

Although the specific contours of the fiduciary relationship may be indefinable in some respects, the relationship is a precursor for fiduciary liability.[256] Therefore, it is often more crucial to determine what the duties giving rise to such liability might be.

In healthcare, fiduciary relationships are connected to three central duties: confidentiality (keeping private details confidential), loyalty (acting in the patient's best interest), and care (choosing the best course of action for

[252] *See infra* Part IV. Broadly applicable fiduciary duties could be recognized in limited circumstances where risk is high, trust is necessary, and specialized expertise is needed.

[253] *See* MILLER, *supra* note 247, at 69.

[254] Paul B. Miller & Matthew Harding, FIDUCIARIES AND TRUST: ETHICS, POLITICS, ECONOMICS, AND LAW 9 (2020); *see* Tamar Frankel, *Transnational Fiduciary Law*, 5 U.C. IRVINE J. INT'L, TRANSNAT'L, & COMPAR. L. 15, 22 (2020).

[255] It should be noted that many members of American society do not view healthcare professionals as individuals to be trusted, given the history of abuse in specific communities. For these communities, trust is not preexisting—it has yet to be built despite the existence of statutorily defined duties. *See infra* note 270.

[256] *See* MILLER, *supra* note 247, at 65.

an individual patient to heal rather than harm).[257] Healthcare is a complex field of expertise, and doctors provide a substantial amount of guidance and action—from diagnosing a patient to offering treatment options to directly treating the patient. Any erosion of trust poses significant risks to not only the field of healthcare but also to human health.

In AI healthcare, however, nearly all of these activities are either performed by a manufacturer's device or with a manufacturer's device. However, manufacturers are not currently fiduciaries, though arguably, they benefit from existing fiduciary relationships. The creators of AI technologies are often not members of the healthcare community at all (or regulated as such).[258] Start-ups, for example, survive through commercialization or licensing the product; the goal is typically to be acquired by a larger medical device manufacturer, sometimes manufacturers that do not have the expertise to create the AI.[259] In some cases, AI technology developers create AI platforms that can then be licensed to medical device manufacturers to create or integrate products.[260]

Although manufacturers may not intentionally "manipulate trust," they nevertheless benefit from false trust.[261] When a fiduciary relationship exists between physicians and their patients, patients rely on physicians to explain potential risks. However, physicians do not often understand how AI medical devices work, and medical device manufacturers that acquire or license

[257] *See* Balkin, *infra* note 290, at 1228.

[258] *The Challenges in Healthcare Technology*, IRONORBIT, https://www.ironorbit.com/the-challenges-in-healthcare-technology/ (last visited Feb. 26, 2023) (describing the emergence of classic technology companies into the healthcare field); *Top Artificial Intelligence Companies in Healthcare to Keep an Eye On*, MED. FUTURIST (Jan. 19, 2023), https://medicalfuturist.com/top-artificial-intelligence-companies-in-healthcare/ (describing Google Health's foray into medical research); Rob Toews, *These Are the Startups Applying AI to Transform Healthcare*, FORBES (Aug. 26, 2020, 10:47 AM), https://www.forbes.com/sites/robtoews/2020/08/26/ai-will-revolutionize-healthcare-the-transformation-has-already-begun/?sh=49238b6a722f (describing the start-ups involved in healthcare AI).

[259] *See* Tschider, *Legal Opacity*, *supra* note 42, at 144 (describing the relationship between start-ups and larger manufacturers for licensing technologies); Ignat Kulkov, *Next-Generation Business Models for Artificial Intelligence Start-Ups in the Healthcare Industry*, INT'L J. ENTREPRENEURIAL BEHAV. & RSCH., Oct. 15, 2021, at 1, 8, 10, https://www.emerald.com/insight/content/doi/10.1108/IJEBR-04-2021-0304/full/pdf.

[260] Adam Bohr & Kaveh Memarzadeh, *The Rise of Artificial Intelligence in Healthcare Applications*, *in* ARTIFICIAL INTELLIGENCE IN HEALTHCARE 25, 27, 31, 39, 43 (Adam Bohr & Kaveh Memarzadeh eds., 2020) (describing examples of platforms adapted for healthcare).

[261] Usually, issues with trust are described as intentional manipulation. *See* WALDMAN, *supra* note 233, at 92. However, the existence of alternative, false trust is a different concern—false trust results from a transfer of trust from a legitimate trust-based relationship to one that carries no fiduciary obligations.

technologies may not be able to explain the AI portion of the technology, either.[262]

This is a function of a few different issues, some discretionary and some non-discretionary on the part of manufacturers. First, some manufacturers and start-ups providing technology to manufacturers may not be willing to disclose details of how the AI works, for fear of destroying trade secret status or confidentiality.[263] Even if such information could be shared, the information that could be most valuable would not actually be from the AI itself, but rather, from broader data collection and use practices, practices which typically are disclosed in much detail in existing privacy notices.[264]

If patients are dependent on their doctor for information about data collection and use that could affect their device use, the doctor would likely be ill-prepared to answer, despite the presence of the fiduciary relationship creating a false sense of security.[265] It may be nearly impossible for a doctor to describe actual risks to the individual.[266]

[262] Liam G. McCoy et al., *What Do Medical Students Actually Need to Know about Artificial Intelligence?*, 3 NATURE PORTFOLIO J. DIGIT. MED., June 19, 2020, at 1, 2, https://www.nature.com/articles/s41746-020-0294-7.pdf.

[263] *See supra* notes 33 (explaining the impediments to data and information sharing with AI systems and applying innovation theories to promote disclosure), 42 (describing the discrete legal choices that organizations may make to protect their investments).

[264] Privacy notices suffer from exogeneity problems. *See* Tschider, *The Consent Myth*, *supra* note 132, at 1524–26. For example, potential risks to the individual are often buried in third-party relationships in ways that may not be known to the organization or person in a relationship of trust. *Id.* Additionally, the development of AI technologies often means that at the moment data are collected, it may be unknown how or to what extent (if at all) those specific data will be useful to the functionality of the AI itself. *Id.* at 1526–27. However, it *may* be known how organizations plan to use such data, but the addition of significant details may make these notices unreasonably long where such notices are difficult to understand from a risk perspective. *Id.* at 1521–23. Further, not all health data uses will be subject to HIPAA notice requirements, creating considerably more latitude in what is actually communicated to downstream users. *Id.* at 1523.

[265] The opacity inherent in AI technologies and buried in layers of third-party data use makes it nearly impossible for a healthcare provider to understand how data will be used and explain it in easy-to-understand language to a patient. AI creates major issues for informed consent, as well.

[266] *See generally* A. Michael Froomkin, *Big Data: Destroyer of Informed Consent*, 21 YALE J. L. & TECH. 27 (2019) (describing the reframing of informed consent under the Common Rule for medical research and its substantial limitations). It should be noted that informed consent and privacy notice and consent are generally considered distinct concepts: Informed consent is based on advice to the patient on risks and benefits of choosing a course of treatment (or not to treat), whereas privacy notice and consent are usually specific to data collection and use. In clinical research under the Common Rule, however, such practices are often combined, with data collection and use practices communicated alongside risk language like “may cause damage to your kidneys.” *See* Tschider, *The Consent Myth*, *supra* note 132, at 1524 (observing that privacy notices rarely communicate in such a way where the individual can assess their potential risks in some salient way); Tschider, *Medical Device Artificial Intelligence*, *supra* note 45, at 1606 (noting that “patients are comparatively in a less beneficial position to appropriately avoid potential risks”).

5. The Choice Paradox: Your Privacy or Your Life?[267]

In the event a patient desires to influence their privacy interests, they are faced with an impossible choice: Do I follow my doctor's orders and live (or improve my quality of life or health outcomes) or choose privacy? In a high-stakes game of adhesive contracting, choice is not a matter of whether to consent to a privacy notice, but whether to use AI medical device technology at all, a concept inherent in adhesive contracting generally.[268]

Choosing to walk away from a comparatively more safe and efficacious surgical procedure is not the same as buying a discretionary consumer product. The stakes are much higher and indeed, the available alternative options may be fewer. When it comes to insurance or Medicaid/Medicare reimbursement, the options may be even more limited. Ultimately, privacy law as it stands is not equipped to tackle the dynamic environment created by AI, primarily framed to focus on individual rights and "choice."[269]

Modern economics, owing much to Vilfredo Pareto, often describes consumer behavior as ranked preferences, or ordinal utility, listing preferences in order with respect to each other.[270] In privacy law, this likely means that there may be individual preferences that rank higher than privacy interests—for example, incentives to exchange data for cash payments,

[267] Ari Ezra Waldman describes the "privacy paradox" wherein individuals care about privacy but do not make decisions in line with these interests. Ari Ezra Waldman, *Cognitive Biases, Dark Patterns, and the 'Privacy Paradox'*, 31 CURRENT OP. PSYCH. 105, 105 (2020). I use the terminology of "paradox" here to describe a kind of super-adhesive contracting relationship—although it may *appear* as if a patient has a choice, the patient actually has no reasonable choice. In these scenarios, a patient must choose between life, or quality of life, and privacy, a Hobson's choice for healthcare.

[268] As Gregory Klass describes, although assent in contract and consent to a privacy notice are distinct legal concepts, they are neighbors. Gregory Klass, *Empiricism and Privacy Policies in the Restatement of Consumer Contract Law*, 36 YALE J. ON REGUL. 45, 93 (2019). In fact, both may relate to data collection and use for AI health devices, especially devices that are consumer-facing that might use both a terms of use document and a privacy notice. However, when AI health devices are used through a health care provider, the provider is usually tasked with effectively informing the individual and soliciting their informed consent and consent to a privacy notice.

[269] *See* Andrejevic, *supra* note 197, at 49.

[270] These preferences are not static: They are animated by community and cultural attitudes and personal experiences. Several examples illustrate a history of inequities and exploitation, which may create a justifiable lack of trust in the medical community. Amongst *many* other examples, see, for example, Elizabeth Nix, *Tuskegee Experiment: The Infamous Syphilis Study*, HISTORY (Dec. 15, 2020), https://www.history.com/news/the-infamous-40-year-tuskegee-study; REBECCA SKLOOT, THE IMMORTAL LIFE OF HENRIETTA LACKS 1–2 (2011); KHIARA M. BRIDGES, CRITICAL RACE THEORY: A PRIMER 335 (2019); Leana Wen, *Doctors' Ignorance Stands in the Way of Care for the Disabled*, NPR: SHOTS (May 17, 2014, 2:13 PM), https://www.npr.org/sections/health-shots/2014/05/17/313015089/doctors-ignorance-stands-in-the-way-of-care-for-the-disabled; KHIARA M. BRIDGES, THE POVERTY OF PRIVACY RIGHTS 5 (2017); VIRGINIA EUBANKS, AUTOMATING INEQUALITY: HOW HIGH-TECH TOOLS PROFILE, POLICE, AND PUNISH THE POOR 83 (2018).

coupons, or better technology offerings. However, in healthcare, these interests are more nebulous. Consider the following scenario:

> *Angel, a privately insured patient with a moderate income who has classically had a strong relationship with the healthcare system, needs an insulin pump to manage their Type-1 diabetes. Angel is presented with two options by their doctor, both insulin pumps that use AI systems. Angel knows that AI collects a lot of data—after all, the pump connects to their mobile device and provides reports to their doctor.*

Even if Angel cares about their privacy and receives accurate information about how their data will be used, it will probably not be enough to forego using the pump or deviate from their doctor's recommendation.[271] Assuming no other considerations go into the decision, such as how much their insurance will pay, Angel will likely proceed. In this scenario, Angel does not really have meaningful choice because the context of making the choice cannot overcome inherent ranked preferences where device quality, safety, efficacy, and out-of-pocket cost, outweigh privacy interests (so long as Angel can understand these practices).

Angel's life experiences, however, could radically change the outcome of this situation in other negative ways. For example, Angel could be receiving public healthcare assistance, such as Medicaid, and Angel's medical device manufacturer could be sharing treatment-related data with Medicaid if required by a government contract. Or the medical device company could sign a private agreement with Medicaid that arranges for greater data sharing in exchange for a lower device cost. If Angel does not want their information shared with the government, Angel may have to pay a substantial amount out of pocket to change insulin pumps.

Angel may also be a member of a community where distrust of the healthcare system is real, and the healthcare system has a history of exploiting people like Angel in the community due to their race, immigration status, income level, disability status, intimate affairs, or identity.[272] In this case, Angel may intentionally avoid a better medical device because the data collected could harm Angel in many other discriminatory ways. Patients like Angel should not have to choose between data use that may introduce substantial privacy risks and safe and efficacious treatment.

In the event medical device choice is not impacted by ranked preference issues, device options may still be comparatively limited. Overall, medical

[271] Information accuracy in economics assumes perfect information, and imperfections in individual notice and consent cannot effectively support ranked preferences. *What is 'Perfect Information'?*, OUR ECONOMY, https://www.ecnmy.org/learn/you/social-influences-culture-information/what-is-perfect-information/ (last visited Apr. 21, 2023).

[272] *See supra* note 270.

devices are high-innovation technologies protected by patents, and the trade secret and confidential status of the AI they include limits the degree to which competitors can enter the marketplace for a given device type.[273] Although these devices are designed to solve the most impossible of healthcare issues, they are also not terribly numerous in options. And few devices today boast enhanced privacy protection as a selling point.

6. Inadequate Privacy as Excessive Exploitative

The cumulative effect of the challenges described thus far is that patients using AI medical devices are very likely to be exploited for their data, data which are highly valuable to an organization. But exploitation on its own is not necessarily *excessive*. Exploitation may not even be holistically harmful to an individual. Understanding the degree of exploitation is essential to determining the appropriate approach to prevent damaging practices.

First, it is important to acknowledge that exploitation may be transactional or structural[274]—exploitation that creates unfairness for device users. Systemic exploitation is reflected in the underlying prevailing issues of false trust, a lack of similarly efficacious alternatives, and ranked preferences.

Exploitation is likely to be transactional as well, as medical device manufacturers rely on procedural privacy fraught with issues, such as an individual reviewing a non-negotiable privacy notice and consenting to it with no other choice. While exploitation stems from unfairness, the combined impact of structural and transactional exploitation creates the possibility of exploitation exceeding standards of reasonableness. Excessive exploitation results from healthcare exploitation when the effect disproportionately affects an individual in comparison to their non-healthcare technology using peers. Furthermore, the way in which an individual is affected may certainly be intersectional in nature.[275]

7. Existing AI Discrimination Concerns

It is well-known that AI can create new discrimination risks based on how data are collected and used, and ultimately, how decisions are rendered. Many scholars, such as Sharona Hoffman, Andrew Selbst and Solon Barocas,

[273] Marta Villarraga & Jorge A. Ochoa, *Trade Secrets in the Medical Device Industry: The Role of Company Documentation*, AM. BAR ASS'N (Dec. 11, 2019), https://www.americanbar.org/groups/litigation/committees/business-torts-unfair-competition/articles/2019/winter2020-trade-secrets-medical-device-industry-documentation/ (describing the competitive medical device environment).

[274] *See* Zwolinski, *supra* note 193.

[275] NANCY LÓPEZ & VIVIAN L. GADSDEN, NAT'L ACAD. MED. PERSPS., HEALTH INEQUITIES, SOCIAL DETERMINANTS, AND INTERSECTIONALITY 1–2 (2016).

Sonia Katyal, Dennis Hirsch, Lilian Edwards and Michael Veale, Ignacio Cofone, and Daniel Schwarcz, have discussed varying AI discrimination problems, including models for resolving issues of transparency and testing to avoid AI issues.[276] As scholars have observed, big data has the potential to perpetuate discrimination,[277] encode existing discriminatory impact (including AI training data),[278] or fail to test for disparate impact.[279] Because big data feed AI algorithms, such discrimination may be opaque, even to an AI's creators.[280] These issues are not unique to general consumer technologies; they also exist in medical device AI.[281]

The preexisting deontological and consequentialist risk presented by healthcare AI may be even more significant for those who may already be at risk for discrimination. For example, a patient who could already be exposed to discriminatory risk of harm simply because the patient is a person of color using AI (that may disproportionately affect specific racial groups) may be exposed to even more risk of harm. Consider the following example:

> *Cace Anurak is a U.S. Marine veteran of Thai descent. Cace suffered spinal injuries in the Iraq war and is tetraplegic. Cace*

[276] *See* Hoffman, *supra* note 33, at 1776–77. *See generally* Sharona Hoffman & Andy Podgurski, *Artificial Intelligence and Discrimination in Health Care*, 19 YALE J. HEALTH POL'Y, L. & ETHICS, no. 3, 2020, at 4, 12–18 (describing the myriad ways in which technology can discriminate against patients due to data and selection bias, feedback loops, and algorithmic functionality); Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671 (2016) (describing the rise of disparate impacts on vulnerable groups as a dominant outcome of big data use with AI); Andrew D. Selbst & Solon Barocas, *The Intuitive Appeal of Explainable Machines*, 87 FORDHAM L. REV. 1085 (2018) (describing the positioning of explainability and transparency as theoretical cures for potential discrimination issues); Dennis D. Hirsch, *That's Unfair! Or Is It? Big Data, Discrimination and the FTC's Unfairness Authority*, 103 KY. L.J. 345 (2014–2015) (describing the use of the FTC's unfairness authority to prosecute potential unfairness issues); Sonia K. Katyal, *Private Accountability in the Age of Artificial Intelligence*, 66 UCLA L. REV. 54 (2019); Lilian Edwards & Michael Veale, *Enslaving the Algorithm: From a "Right to an Explanation" to a "Right to Better Decisions"?*, INST. ELEC. & ELECS. ENG'RS SEC. & PRIV., May–June 2018, at 46; Tschider, *Regulating IoT*, *supra* note 51; Ignacio N. Cofone, *Algorithmic Discrimination Is an Information Problem*, 70 HASTINGS L. J. 1389 (2019); Andrew D. Selbst et al., *Fairness and Abstraction in Sociotechnical Systems*, *in* ASS'N FOR COMPUTING MACH., FAT* '19: PROCEEDINGS OF THE 2019 CONFERENCE ON FAIRNESS, ACCOUNTABILITY, AND TRANSPARENCY 59 (2019); ALEX ROSENBLAT, TAMARA KNEESE & DANAH BOYD, DATA & SOC'Y RSCH. INST., ALGORITHMIC ACCOUNTABILITY (2014), https://datasociety.net/pubs/2014-0317/AlgorithmicAccountabilityPrimer.pdf; Daniel Schwarcz, *Health-Based Proxy Discrimination, Artificial Intelligence, and Big Data*, 21 HOUS. J. HEALTH L. & POL'Y 95 (2021).

[277] *See* Cofone, *supra* note 276, at 1399–405 (describing discrimination via discriminatory data, encoded bias, and bias in process).

[278] *Id.*

[279] *See* Selbst & Barocas, *supra* note 276, at 1130 (describing the information needed to evaluate models for disparate impact).

[280] *See* Cofone, *supra* note 276, at 1437 (explaining that opacity is a key concern for evaluating consequences of AI decisions).

[281] *See* Tschider, *Medical Device Artificial Intelligence*, *supra* note 45, at 1606.

> *received a spinal cord stimulator and electronic array, trained by AI and implanted in his spine and brain, respectively. The stimulator connects and interprets spinal cord messages across spinal lesions to restore ambulatory function. The AI, however, has only been trained on Caucasian test subjects, test subjects who also were not exposed to conditions Cace suffered after his injury in a war zone. As a result, Cace has experienced extreme pain while using the stimulator.*

In the example above, Cace's Thai heritage may not have directly caused the painful outcomes he is experiencing. However, if data used to train AI algorithms powering the stimulator are not representative of potential user groups of varying racial or ethnic backgrounds, devices like this could carry a larger risk of harm to Cace and other patients like him. In this example, not only might Cace be exposed to deontological and consequentialist harms due to data collection and overuse, Cace might also face potential safety issues because the device itself was not trained on representative data from other users from the same race, ethnicity, or geographic community.

Although all medical device users may be exposed to excessive exploitation, preexisting risks of discrimination based on lack of *representative* data mean that members of underrepresented communities face even more risk than their represented counterparts.

8. Excessive Exploitation

In addition to groups already exposed to discriminatory risk, patients using compulsory medical devices cannot reasonably avoid deontological risk of harm, creating substantial, and sometimes pervasive, harm. For these technologies to work safely and efficaciously (as described in Part I), they likely require ubiquitous, continuous, and sensitive data collection, increasing the probability of excessive exploitation.

When large volumes of data are collected, organizations may wish to duplicate, amend, share, or sell such data. Therefore, from a deontological risk of harm perspective, patients using many AI-enabled medical technologies will collectively be subjected to substantial privacy risk and surveillance, whereas their peers will not, often without even knowing it. Patients may not become aware of such incendiary practices until consequentialist risk becomes a reality, such as if identity theft or insurance fraud occurs.

In this way, limiting data collection and use is tremendously difficult to achieve because data are essential to AI functionality. The opacity of how AI make decisions with respect to these data further limits how patients can understand how and to what extent their data are used. Finally, when data are disembodied from the individuals creating data through human-computer collaboration, the risk of overuse increases substantially.

9. *Fiduciary Duties Foundational to Overcoming Excessive Exploitation*

The underlying foundation for all relationships, including those involving AI medical devices, is trust. Patients rely on doctors with whom they have a relationship of trust, but the trust is misplaced when it is inappropriately transmitted to manufacturers and technology providers that are not included within this fiduciary relationship.[282]

The nature of the relationship between a patient and a manufacturer or technology provider *would* be fiduciary in nature if a doctor were providing the technology or service rather than a device manufacturer. The problem, though, is a fiduciary relationship generally is not applied broadly, as it is usually defined statutorily.[283] And in many cases, manufacturers likely would not perform the role of a fiduciary despite calling some devices “robot doctors” or similar.

A broadly applicable fiduciary relationship, such as an information fiduciary, should attach to a relationship when the potential risk of harm is significantly high. Otherwise, the role of a fiduciary, especially when other important fiduciary relationships exist, risks losing its importance. When everyone is responsible, no one is responsible.

Fiduciary relationships are crucial to the trust of an overall system, and when an individual cannot trust their fiduciary, confidence in the system or sector as a whole diminishes. Moreover, a lack of alternative technologies or equivalently effective technologies forces patients to make choices that deprioritize privacy considerations and increase the potential for misuse. When confronted with a serious health condition, patients would likely choose health before privacy.

D. Demonstrating Excessive Exploitation

When all or most of these nine factors are present, individuals cannot meaningfully protect their data interests, resulting in exploitationwhen AI

[282] Discussions of fiduciary duty primarily focus on the doctor-patient relationship, and usually the focus is on a doctor’s fiduciary duty to a patient, not any relational duties between them or any entities outside of that specific relationship. *See* W.A. Rogers, *Is There a Moral Duty for Doctors to Trust Patients?*, 28 J. MED. ETHICS 77, 77–78 (2002).

[283] Gregory S. Alexander, *A Cognitive Theory of Fiduciary Relationships*, 85 CORNELL L. REV. 774, 776–77 (2000) (describing the special legal distinction given to certain relationships that are subject to “more stringent legal norms”). These relationships and their obligations, however, are highly contextual, specific to the two parties involved.

medical device-using patients are exposed to significantly more privacy risk than their peers.[284]

On balance, risk to individuals reliant on frequent healthcare or compulsory medical devices are more exposed than their peers who are not reliant. Most if not all of this healthcare use is compulsory in nature, and there is no real choice possible in whether to provide or not provide data. This collective increased deontological (and, likely, consequentialist) risk creates excessive exploitation.

IV. PREVENTING EXCESSIVE EXPLOITATION

As early as 2001, Ian Kerr proposed that holding information could create some reciprocal responsibility in a fiduciary relationship.[285] The information fiduciary movement calls for the creation of a duty of loyalty for all information collectors.[286] Simply by collecting personal information, a fiduciary duty is created. An information fiduciary primarily owes a duty of loyalty and confidentiality to the individuals whose data the fiduciary solicits or collect, which is a limited duty compared to preexisting fiduciary relationships. In healthcare fiduciary relationships, a duty of loyalty is not the only relevant duty. For example, a duty of care and duty of expertise accompany duties of loyalty and confidentiality that require a physician to act in the best medical interest of a patient. Specifically for the healthcare sector, where fiduciary relationships are already reasonably expected,[287] an information fiduciary role that acknowledges the realities of a digital world could enhance "dividual privacy" goals.[288] As John Cheney-Lippold describes this new world, we must embrace the new world of privacy while promoting individual interests, as well:

[284] *See* Zuboff, *supra* note 209, at 186–87.

[285] Ian R. Kerr, *The Legal Relationship Between Online Service Providers and Users*, 35 CANADIAN BUS. L.J. 419, 446–57 (2001).

[286] Adam Schwartz & Cindy Cohn, *"Information Fiduciaries" Must Protect Your Data Privacy*, ELEC. FRONTIER FOUND. (Oct. 25, 2018), https://www.eff.org/deeplinks/2018/10/information-fiduciaries-must-protect-your-data-privacy. All fiduciary duties have a duty of loyalty at their center. Deborah A. DeMott, *Breach of Fiduciary Duty: On Justifiable Expectations of Loyalty and Their Consequences*, 48 ARIZ. L. REV. 925, 935 (2006).

[287] Fiduciary relationships are generally expected due to the obligations between doctor and patient and enhanced obligations for insurers at the state and federal level. These existing relationships mean that an information fiduciary role for organizations within the healthcare ecosystem may not be unexpected, at least from the perspective of a patient.

[288] JOHN CHENEY-LIPPOLD, WE ARE DATA: ALGORITHMS AND THE MAKING OF OUR DIGITAL SELVES 236 (2017). Dividual privacy is defined as "a privacy that extends beyond our individual bodies, that accepts the realities of ubiquitous surveillance, and that defends the 'right to be let alone' even, and especially, when we are made of data—because the teeth of its liberal cousin cut too superficially and inefficiently." *Id.*

> We need dividual privacy—a privacy that extends beyond our individual bodies, that accepts the realities of ubiquitous surveillance . . . . To anoint the individual subject as the sole index of power is to miss out on everything else that happens outside the individual's point of view . . . . Understanding that our data is part and parcel of who we are and what we are subject to lets us think about privacy in a new way.[289]

Essentially, dividual privacy creates the *right* incentives and regulatory structures while embracing the realities of legitimate and sometimes beneficial surveillance. AI medical devices differ from general consumer products in that they have the potential to revolutionize medicine for the better, to democratize access, and to even facilitate personalization that improves healthcare equity. Doubling down on failing privacy frameworks will both reduce the safety and efficacy of desperately needed products and services while failing to dismantle the hidden, exploitative, and potentially discriminatory practices of commercial medical device manufacturers and their third parties.

If an information fiduciary role is intended to be effective, a statutorily created role must be sufficiently definite and not replicate existing issues within the current privacy system. In particular, where existing fiduciary relationships exist, the role must be clearly demarcated and not duplicative of known fiduciary relationships, such as doctor-patient or therapist-patient relationships.

Specifically, information fiduciaries should have a positive obligation to illustrate how exploitation of patients, which *will* occur due to the commercial nature of AI medical device sales, does not amount to excessive exploitation. This Part aims to briefly introduce one potential model for better addressing exploitation issues. It is intended to explore, at a high level, how we can begin to conceptualize exploitation problems differently by applying an information fiduciary role and attendant *ex ante* obligations to AI medical device manufacturers.

A. Contours of An Information Fiduciary

Jack Balkin reintroduced the concept of an information fiduciary in 2016, to varying degrees of support.[290] Balkin's description of the role stemmed from data's application to robotics and big data.[291] The three laws,

[289] *Id.*

[290] Jack M. Balkin, *2016 Sidley Austin Distinguished Lecture on Big Data Law and Policy: The Three Laws of Robotics in the Age of Big Data*, 78 OHIO ST. L.J. 1217 (2017).

[291] *Id.*

explained below, reflect the realities of AI and big data, illustrating many of the problems described herein.[292]

First, Balkin described that "algorithmic operators are information fiduciaries with respect to their clients and end-users."[293] This concept is illustrative of the power dynamics implicit in these relationships: One organization presumably has access to and can control (at least to some degree) how opaque AI systems work and the effect these systems have on individuals.

Factually speaking, certainly this is true, but it could also be argued that this relationship alone would exist for generalized concepts of duty, as in negligence, for example in the undertaker's duty. The undertaker's duty is typically a plaintiff's response to a defendant's complete defense that no individual has a positive duty to help another. The undertaker's duty applies when a defendant has voluntarily provided assistance to someone, has "undertaken" a duty that would not otherwise be owed to the other.[294] Then, if the individual stops performing the duty, the other individual would be left in a worse position than when the first party undertook the duty.[295]

There may be scenarios where AI system opacity is innocuous and scenarios where opacity is such a significant problem that a positive fiduciary role is necessary. Moreover, AI may be highly procedural and not likely to inspire confidence or trust. Without knowing the context of the situation, it is difficult to distinguish when a positive duty, as in an information fiduciary, should apply.

Second, Balkin specifies that algorithmic operators have a duty toward the general public.[296] Balkin specifically describes the role of bystanders and other individuals who are not in privity with a manufacturer but who are nevertheless harmed by defective products.[297] Although this concept ties more directly to questions of liability for consequential risk of harm, the concept also illustrates the larger environment in which AI systems operate. For example, a loss of trust can result in distrust of the overall system, a system that already is rife with legitimate community-based distrust.[298] The

[292] *Id.*

[293] *Id.* at 1227.

[294] RESTATEMENT (SECOND) OF TORTS § 323 (AM. L. INST. 1965).

[295] Balkin, *supra* note 290, at 1227.

[296] *Id.* at 1231.

[297] *Id.* at 1232.

[298] *See, e.g.*, Martha Hostetter & Sarah Klein, *Understanding and Ameliorating Medical Mistrust Among Black Americans*, COMMONWEALTH FUND (Jan. 14, 2021), https://www.commonwealthfund.org/publications/newsletter-article/2021/jan/medical-mistrust-among-black-americans; Bernice Roberts Kennedy, Christopher Clomus Mathis & Angela K. Woods, *African Americans and Their Distrust of the Health Care System: Healthcare for Diverse Populations*, 14 J. CULTURAL DIVERSITY 56 (2007); Lauren Vogel, *Broken Trust Drives Native*

problem is so endemic to healthcare that it is possible that increasing trust-based relationships where organizations are actually held to their obligations could work to improve the system, if trust is taken seriously and excessive exploitation is avoided.

Finally, Balkin relates a third law, that "algorithmic operators have a public duty not to engage in algorithmic nuisance."[299] Such algorithmic nuisance is described as engaging in harmful behavior, diffusing harm over an indefinite population.[300] Balkin describes such a nuisance in relation to Andrew Selbst's description of intentionality in algorithmic discrimination: Namely, that intent is not the appropriate barometer for discrimination—an algorithm cannot *intend* to discriminate.[301] Rather, it encodes certain behaviors that render a social effect, and whether such effects are justified.[302]

This concept relates to the reality of AI medical device exploitation, importantly that exploitation may be endemic to the macroeconomic marketplace and capitalistic dynamics—power differentials and information asymmetries may be unavoidable. However, the *effects*, in particular the combined effects for individuals, communities, and the market overall could justify additional duties on behalf of AI medical device manufacturers.

Frank Pasquale has commented on Balkin's work, importantly adding an additional law of robotics to consider, while cautioning on the third law's applicability.[303] Pasquale specifically describes an "attribution problem," or the challenge of regulating machines without ascribing some legal responsibility to one or many persons, natural or commercial in nature.[304] Indeed, the evolution of AI development could exceed the original creator's intention, through continuous learning of the technology itself or use of the

Health Disparities, 187 CANADIAN MED. ASS'N J. E9 (2015); C.L. Sung, *Asian Patients' Distrust of Western Medical Care: One Perspective*, 66 MOUNT SINAI J. MED. 259 (1999); Amanda Machado, *Why Many Latinos Dread Going to the Doctor*, ATLANTIC (May 7, 2014), https://www.theatlantic.com/health/archive/2014/05/why-many-latinos-dread-going-to-the-doctor/361547/; C.O. Cunningham et al., *HIV Status, Trust in Health Care Providers, and Distrust in the Health Care System Among Bronx Women*, 19 AIDS CARE 226 (2007). These articles are some of countless articles and only begin to scratch the surface of trust issues amongst many U.S. residents.

[299] *See* Balkin, *supra* note 290, at 1232.

[300] *Id.* at 1232–33.

[301] *Id.* at 1233–34.

[302] *Id.* at 1234. Pasquale has described the reasonable limitations of a law of nuisance, importantly noting that the well-known nature of discriminatory impact within algorithmic design may result in actual liability in limited circumstances, rather than only a broad social impact. *See* Pasquale, *supra* note 19, at 1249. Although this Article does not delve into the details of tort liability for AI, this caution is an important check on unlimited and broad social liability when more specific applications might make sense. This overall caution certainly motivates limiting the application and scenarios in which an information fiduciary role is recognized.

[303] Pasquale, *supra* note 19, at 1249, 1252–53.

[304] *Id.* at 1252–54.

application in unexpected ways. For example, the AI could be licensed for use with a variety of different devices or the AI company could be acquired by another organization. Ultimately, establishing fiduciary duty could be challenging when the duty's scope changes over time—so fiduciary duty is not static but likely flows with the technology itself.

Balkin has expanded the concept further, applying the information fiduciary concept to privacy law.[305] The frame for such an application is very similar to the concepts described in Part III, namely that surveillance capitalism spurs digital dependence, and such dependence requires additional corresponding responsibilities.[306] Balkin succinctly summarizes the broader problem, noting that:

> Although digital companies know a lot about us, we do not know a lot about them —their operations, what kinds of data they collect, how they use this data, and who they share it with. Because of this asymmetry of information, we are especially vulnerable to them, and we have to trust that they will not betray our trust or manipulate us.[307]

As Balkin further notes, the issue is not simply asymmetry, it is that digital companies want consumers to use their products, so much of the communication prompts individuals to lean into technology, to make technology part of everyday life, prompting individuals to provide more information.[308] As described in relation to the Livio hearing aid, certain technology affordances and ease of use similarly promote reliance and provision of additional data sources, such as the Livio's integration with a mobile device music playlist or health apps.[309] Such devices also direct attention to lifestyle benefits rather than details about how the technology works or the data they collect.[310] The collective impact is that these devices function based on users providing more data, not less.

Finally, in responding to criticism regarding the fiduciary model, Balkin notes that the function of a fiduciary has the potential to overcome broader competition issues.[311] As described in Part III, one underlying competition issue for AI medical devices is the lack of comparable alternatives in the marketplace, as well as forces that direct an individual toward digital devices, such as a physician's standard of care, insurance coverage, or public health assistance, such as Medicaid or Medicare coverage.

[305] Jack M. Balkin, *The Fiduciary Model of Privacy*, 134 HARV. L. REV. F. 11 (2020).

[306] *Id.* at 11.

[307] *Id.*

[308] *Id.* at 12.

[309] *See supra* notes 97–100 and accompanying text.

[310] *See supra* note 9.

[311] *See* Balkin, *supra* note 305, at 21.

These forces, which may have a substantial impact (if a patient opts for a device that is not reimbursable through insurance) along with demonstrated health concerns (creating a sense of exigency in making a decision), outweigh privacy interests when an individual engages in preference ranking.

The information fiduciary model may be broad in nature, but for AI medical devices, this model may be useful. In establishing an information fiduciary role for such manufacturers, however, a critical question is *how* manufacturers can demonstrate duties of loyalty and care with respect to patients, especially when a physician is usually prescribing the device (as in DreaMed AdvisorPro) or using the device in conjunction with the patient (as in surgical robotics like the CyberKnife).

B. How the Information Fiduciary Duty of Loyalty and Care Might Be Demonstrated

Recognizing the role of an information fiduciary acknowledges and names the increased risk to individuals otherwise dependent on healthcare technologies and protects their interests. This section only begins to explore how a fiduciary role could work for AI medical device manufacturers.

As Richards and Hartzog note, where vulnerabilities are low, either because there is currently a small amount of trust required or where there is low risk of exposure, duties of care and loyalty might be similarly diminished.[312] However, where vulnerabilities are high, higher duties of care and loyalty might be required.[313] It is precisely this context that reflects the reality of information transactions. In healthcare specifically, scenarios that substantially increase deontological risks of harm related to excessive exploitation should demand a greater duty of care and loyalty.

Initially, the information fiduciary role could be narrowly tailored to sectors and scenarios like healthcare, where the deontological (and, potentially, consequentialist) risk of excessive exploitation is inherently high. Creating an obligation might be most appropriate at the state level, where fiduciary relationships are largely defined. For example, state healthcare privacy laws could explicitly designate the fiduciary role and to whom it applies, even establishing fiduciary obligations in scenarios where AI are used.[314] Such obligations should be published separately and distinguished

[312] *See* Richards & Hartzog, *Taking Trust Seriously*, *supra* note 233, at 458. Richards and Hartzog propose an alternative description of Discretion, Honesty, Protection, and Loyalty as defining factors for establishing trust in these scenarios. *Id.*

[313] *Id.*

[314] A wide variety of healthcare privacy laws currently exist, and to avoid preemption, it might be desirable to frame these obligations as responding to privacy rather than product safety concerns. For example, Maryland permits disclosure to third parties when the patient's identity is not revealed through the records. A law like this could be used to expand access to healthcare data. Similarly, laws like Colorado's new privacy law, the Colorado Privacy Act, requires substantially more

from general tort obligations which might be preempted under FDA medical device preemption.[315]

Moreover, the benefit of identifying an information fiduciary role is that harms are reconceived based on duties of loyalty and care. Risk of harm, therefore, including deontological and consequentialist risks of harm, may be sufficient to illustrate when an organization has not effectively performed their duties, rather than the comparatively higher standard of legal injury that applies to common law torts. This model works more effectively for information harms that may be hard to prove. Fiduciary duties, therefore, can be tied to statutorily defined harms, or may be focused on prescriptive duties themselves.

Federal healthcare privacy laws seem to offer some opportunity for additional responsibilities in this space as well. First, organizations that are not directly regulated by HIPAA may now be regulated. Second, organizations that are currently regulated by HIPAA will not be preempted by additional regulation: HIPAA is a floor, not a ceiling, and carries no express preemption clause, barring only laws directly in conflict with HIPAA.[316] Finally, failure to fulfill a fiduciary duty statutorily could be referred to a state attorney general's office or similarly construed to demonstrate unfair or deceptive trade practices, which would be similar to how many information practices are enforced today.[317]

Several models could be applied to demonstrate fulfillment of fiduciary duty. For example, conducting HIPAA risk assessments and posting them publicly on an HHS website could count, or increasing salient details in a website-hosted privacy notice (including identities and locations of third parties, or commercial entanglements) certainly could illustrate some additional transparency. Other examples could include involving patients in focus groups and feedback sessions on information handling practices, as the EU has required under the General Data Protection Regulation.[318]

privacy-protective steps by any organization collecting personal information in Colorado. Similar laws could be passed specific to healthcare AI and privacy. MD. CODE ANN., INS. §§ 4-403(b), 14-138(b) (2023); Colorado Privacy Act, ch. 483, 2021 Colo. Sess. Laws 3445.

[315] *See generally*, Tschider, *Medical Device Artificial Intelligence*, *supra* note 45 (describing a history of SCOTUS preemption decisions and the likely and dangerous expansion into medical device AI).

[316] Joy Pritts, *Preemption Analysis Under HIPAA: Proceed with Caution*, AM. HEALTH INFO. MGMT. ASS'N: IN CONFIDENCE (Apr. 14, 2003), https://library.ahima.org/doc?oid=59816#.ZCPQl8LMKM8.

[317] Charlotte A. Tschider, *Experimenting with Privacy: Driving Efficiency Through a State-Informed Data Breach Notification and Data Protection Law*, 18 TUL. J. TECH. & INTELL. PROP. 45, 70–71 (2015). *See generally* CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY (2016).

[318] Regulation (EU) 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free

One of the most powerful activities that an organization can do, however, is to conduct legitimate interest analysis.[319] Legitimate interest analysis explicitly requires organizations engaging in behaviors that substantially increase risk to the patient to identify the interests of the patient, community, or broader public health and the interests of the organization.[320] A legitimate interest analysis is performed using a repeatable format, taking into account commercial financial interests, potential downstream benefits, and community or public health activities.[321] The goal in conducting such an analysis is to determine whether substantial deontological harms might emerge from seemingly justifiable personal information collection and use.

This assessment is designed to demonstrate fulfillment of a fiduciary duty of loyalty. A legitimate interest analysis might complement other privacy activities but expands the notion of privacy into a model that includes power dynamics, consumer health market dynamics, and potential commercial benefits related to data collected. A legitimate interest analysis could also closely scrutinize data collection and use through the lens of minimum necessary, for example, permitting collection and use when it is narrowly tailored to the interests of the individual and their use of the specific technology. A legitimate interest analysis would enable organizations to avoid excessively exploitative behaviors by centering the individual's interests rather than satisfying a checklist of privacy requirements.[322]

Creating an information fiduciary role for manufacturers of health technology or extending the healthcare fiduciary role further than between doctors and their patients has the potential to reduce both deontological harms and consequential risks of harm. Although an individual may lose some ability to individually negotiate, their interests must be evaluated from the point of data collection and the potential for coercion by an organization collecting such data.

This approach reframes healthcare relationships from individual to collective without adopting a completely utilitarian point of view, where the ends justify the means and individuals are more likely to be excessively exploited. This model reinforces the idea that as the more powerful and knowledgeable party, a manufacturer owes a duty of loyalty to a patient. Practically, data collection or use inconsistent with substantial benefit to the individual will not likely pass muster. However, substantial benefit to the

Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1.

[319] *See* Tschider, *AI's Legitimate Interest*, *supra* note 178, at 178.

[320] *Id.*

[321] *Id.*

[322] *Id.* at 180–83.

individual and to a community of individuals like them potentially could justify additional processing.[323]

The European Union's Article 29 Working Party's 2014 Legitimate Interest Opinion offers some direction for this analysis, including consideration of potential individual, class, community harms, negotiation power, information asymmetries, data types, manner of processing, and reasonable expectations of the individual.[324] This analysis can then be posted publicly for purposes of public evaluation.

Legitimate interest analysis is designed to be performed *ex ante* as part of a regulatory regime prior to engaging in data collection or use to prevent deontological harm. Failure to complete such an analysis or relying on an unfavorable analysis demonstrating excessive exploitation could give rise to some responsive legal action. Although today, common law privacy harms do not generally extend to autonomy harms, certain actions could be enforced by the Office for Civil Rights (the enforcement arm of HIPAA), the Federal Trade Commission, or state AGs under a suit either involving the breach of a fiduciary duty or unfair or deceptive trade practices.

This Section only begins to introduce potential avenues for demonstrating fulfillment of an information fiduciary's duty. Although this might be accomplished in multiple ways, potential recommendations should consider how this fiduciary duty can be validated and disseminated to provide an avenue for review, and when necessary, enforcement against excessively exploitative practices.

CONCLUSION

The advent of medical device AI brought with it tremendous promise to democratize medicine and improve human health. But it also brought with it a more pervasive and insidious form of commercial exploitation, central to surveillance capitalism. This Article has described the ways in which exploitation may be excessive in healthcare specifically, where individual

[323] Centering on an individual avoids a solely utilitarian-style public interest that could exploit some individuals while benefiting others. However, a legitimate interest model has the ability to extrapolate the individual inquiry across a population of patients, anticipating and preventing excessive exploitation. This model, then, reduces deontological harms while also reducing consequential risks of harm and balancing potential benefits to an individual, class of individuals, or community. The public interest perspective is very valuable, but public interest versus individual autonomy need not be a dichotomy at all. *Cf.* Sharona Hoffman & Andy Podgurski, *Balancing Privacy, Autonomy, and Scientific Needs in Electronic Health Records Research*, 65 SMU L. REV. 85, 124 (2012) (arguing that in clinical research, when humans are not the subject of physical or psychological testing, common good should prevail over individual interests).

[324] *See Opinion of the Article 29 Data Protection Working Party on the Notion of Legitimate Interests of the Data Controller Under Article 7 of Directive 95/46/EC*, No. 06/2014, 844/14/EN WP 217, at 3, 37–41 (Apr. 9, 2015).

exploitative events and factual circumstances collectively demonstrate that patients have very little choice regarding their data.

First, the patient is in a relationship with their doctor but is using a device (or has a device used on them) created by a manufacturer collecting and using personal information about them. The presence of a fiduciary relationship in this scenario benefits the manufacturer by capitalizing on the preexisting relationship of trust, or false trust.[325] Second, the patient likely requires the device to live or have some quality of life, and there may be few or no alternatives, especially technologies that will be paid for by government entities or private insurance providers. Finally, in order for devices to work safely and fairly, they require continuously provided, sensitive personal information, data that is opaquely processed.[326]

These circumstances demonstrate the complexity of preventing excessive exploitation and illustrate why a patient increasingly must choose their privacy or their life. Today, the only real alternative to avoiding exploitation and preserving individual privacy is not to use the device at all, an adhesive choice that may not be remotely reasonable for patients compulsorily reliant on a medical device. To prescribe a medical device today means exposing a patient to excessive exploitation.[327]

Although commercial exploitation in healthcare is to some extent inevitable due to inherent information asymmetries, differences in expertise, and adhesive contracting limitations, the United States can limit the degree of exploitation that is acceptable. Without an appropriate check on such exploitation, these practices could lead to broader impacts not just to the individual but to community trust in the medical community. A vulnerable person dependent on the medical community for effective medical care should not be excessively exploited simply because they have a health event requiring care.

This Article only begins to explore potential avenues for potential regulatory solutions, but the information fiduciary role holds some promise for expanding the existing fiduciary relationship and avoiding false trust.[328] If organizations are required to conduct assessments that explain their data handling choices from the perspective of a fiduciary, it may be possible to determine where such practices are excessively exploitative.

By identifying, and potentially prosecuting, excessive exploitation by establishing information fiduciary roles in the AI medical device community through laws like HIPAA and more explicit FDA CFR requirements, the United States can better balance justifiable interests in health data collection

[325] *See supra* Section III.C.

[326] *See supra* Part III.

[327] *See supra* Section III.C.5.

[328] *See supra* Section IV.B.

and use with the interests of the individual, creating a symbiotic system that benefits all parties.