NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
VOLUME 25, ISSUE 2: DECEMBER 2023

DIGITAL TWINS IN HEALTHCARE: PROACTIVE REGULATION TO PREVENT A "RUNAWAY TRAIN"

Brynn Story*

This Article explores the implications of integrating digital twins in healthcare, emphasizing the challenges of data breaches and patient privacy. It advocates for proactive legislation to safeguard patient data security, proposing patient-controlled access through blockchain technology. It also underscores the necessity of protecting patient rights, especially in the face of genetic discrimination and criminalized healthcare. Assessing the inadequacies of current legal approaches, this Article suggests a presumption of harm and a private cause of action for data breaches. It emphasizes the urgency for comprehensive regulatory data security frameworks to address societal implications, highlighting the critical need for a robust legal foundation to ensure patient trust and data security in the evolving landscape of medical digital twins.

TABLE OF CONTENTS

I. INTRODUCTION 316
II. BACKGROUND 318
A. Digital Twins' Emerging Role in Healthcare 318
B. The Prevalence of Medical Data Breaches and the Implications for Patients 323
C. Current State of Regulation for Data Privacy in Healthcare 325
III. INEFFICACY OF CURRENT LAW ON DIGITAL TWINS IN HEALTHCARE 326

* J.D. Candidate, University of North Carolina School of Law, 2025. The Author would like to thank the NC JOLT Editors and Leadership, Austin Kamer, Hayfa Ayoubi, Julia Rhys Vaughan-Jones, and McGee Roman in particular. The Author would also like to extend a special thanks to Nigel Story, Bobby Cameron, and Shreeva Adhikari for their unwavering support and guidance.

IV. IMPORTANCE OF PATIENT AGENCY IN DATA PRIVACY 328
A. Defining Data Ownership 329
B. Mitigation of Data Privacy Threats 331
C. Patient Agency Through Proper Causes of Action 333
V. REGULATORY STAKES AND DIRECTION FOR THE FUTURE ...335
A. Importance of Proactive Regulation Against Harm 336
B. Potential Proactive Policy 341
C. Preventing Entrenched Harm Outweighs Legal Overbreadth and Technological Restriction 342
VI. CONCLUSION 343

I. INTRODUCTION

There is a world, not far off from the present one, where cancer has lost its teeth, where doctors can predict the presence of microscopic cancer cells before they metastasize, where chemotherapy treatments can be specifically prescribed based on a patient's exact immune system response, and where a surgeon can plan and practice based on your unique internal physiology from a three-dimensional ("3D") model before they enter the operating room.[1] While this may sound like a world born of science fiction, emerging digital twin technology has the potential to make it our reality. Digital twins, "living" digital models of something in the real world,[2] are the culmination of big data, simulation, and artificial intelligence, and when applied in healthcare, they stand to revolutionize preventative care and precision diagnostics.[3] But with such leaps in progress come leaps in risk, particularly in the domains of data security and patient privacy. The emerging use of digital twins in healthcare opens new doors for hackers to access patients' most sensitive personal data; it has the potential to exacerbate existing issues, like genetic discrimination; and, particularly in the

[1] Tianze Sun et al., *Digital Twin in Healthcare: Recent Updates and Challenges*, DIGIT. HEALTH, Jan. 2023, at 4.

[2] *What is a Digital Twin?*, IBM, https://www.ibm.com/topics/what-is-a-digital-twin#:~:text=Michael%20Grieves%20(then%20on%20faculty,digital%20twin"—in%202010 [https://perma.cc/U7LZ-QV7R] (last visited Nov. 1, 2023).

[3] *See* Mohsen Attaran & Blige Gokhan Celik, *Digital Twin: Benefits, Use Cases, Challenges, and Opportunities*, DECISION ANALYTICS J., Jan. 2023, at 5–6.

post-*Dobbs* era in which states have begun criminalizing certain healthcare, it has the potential to put patients' privacy and livelihood at extreme risk. Fundamentally, if the use of digital twins in the healthcare industry is not properly regulated, it could erode one of the foundational underpinnings of a well-functioning healthcare system: patient trust.

Trust is the cornerstone of modern medicine. As patients, each person wants to trust that every available resource will be exhausted for their care, with no new technology being spared to heal and keep them well. Equally important is the trust a patient places in their healthcare provider to protect the sensitive, personal information conveyed during the medical process: that it will be kept secure, confidential, and used only to provide continuing care to that specific patient. The American medical industry also claims to hold these values to a high standard: ultimate confidentiality along with cutting-edge treatment.

As healthcare merges increasingly into the digital space and new technologies, like personal-data-heavy digital twins, become the future of patient agency and efficient care, data breaches threaten confidentiality and regulations lag behind. This Article argues that to protect patient data security amid rapid advancements in digital twin technology, proactive legislation must create a safer framework for digital twins in the medical space through stricter data security requirements for healthcare providers and a clear cause of action for patients subject to negligent maintenance of their digital twin.

Part II of this Article provides a brief overview of digital twins in the medical space, background on the trend of medical data breaches, and the current state of regulation for data privacy in healthcare. Part III examines the effects of present law as the increasingly sensitive data of digital twins emerges in the medical field, while Part IV discusses how patient agency in owning and controlling their own medical data may help to offset the issues arising from data breaches. Finally, Part V will look at potential steps for lawmakers to preempt harm from data breaches in the future.

II. BACKGROUND

To understand how a technology that has yet to be fully implemented—such as digital twins in the medical space—will interact with the American legal system, it is crucial to have familiarity with existing information in regard to digital twins; evidence of potential threats, like data breaches, based on the use of digital twins in healthcare; and situations where the law has dealt with comparable threats. This Section consists of an overview of digital twins as a technology and their potential uses in healthcare, an exploration of the medical industry's current troubles with data security and its effects on patients, and a general discussion of where American regulations and courts sit concerning data security in healthcare.

A. Digital Twins' Emerging Role in Healthcare

While still a comparatively recent technology overall, digital twins have already made inroads in other industries, offering insights into their potential application in healthcare. A digital twin is a "living" digital replica of a physical entity.[4] As suggested by the definition, there is more to a digital twin than simple digital replication: the word "living" confers the close, interconnected nature of a digital twin to its physical counterpart.[5] Through the use of advanced sensors and monitoring systems, digital twins continually evolve to reflect real-time changes to the physical entity, allowing for the continuous prediction of potential future states.[6] Things that have been modeled with digital twin technology so far include devices or machines, like an aircraft engine, or industry-scale infrastructure and processes, like industry plants or power

[4] Radhya Sahal et al., *Personal Digital Twin: A Close Look into the Present and a Step Towards the Future of Personalised Healthcare Industry*, SENSORS, Aug. 2022, at 1.

[5] Eugen Octav Popa et al., *The Use of Digital Twins in Healthcare: Socio-Ethical Benefits and Socio-Ethical Risks*, 17 LIFE SCI., SOC'Y & POL'Y 1, 2 (2021).

[6] Sun et al., *supra* note 1, at 8.

grids.[7] The use of digital twins was arguably[8] pioneered by the National Aeronautics and Space Administration ("NASA") in the 1960s, replicating space voyages in earth-bound settings.[9] However, the first credited digital twin model was created by Dr. Michael Grieves in 2002 in the manufacturing industry,[10] with NASA coining the term "digital twin" in 2010.[11]

Where digital twins stand out is in their ability to model highly complex and capital-intensive entities, with a specialty in preventative maintenance.[12] Access to a model that is more than a snapshot in time, but rather a "breathing" version of the real thing, amplifies the strength of potential maintenance by allowing scenario-specific experiments without real-world consequences.[13] What makes this aspect of a digital twin work is the flow of information produced by the physical or "real" entity and communicated to the digital twin. The continuous flow of data allows for an essentially live feedback loop enabling ongoing recommended actions or predictive problem solving.[14] Having detailed, live digital replicas of these types of entities that are enhanced by simulation and artificial intelligence allows companies to mitigate or prevent costly losses of real-world functionality, making the effective use of digital twins highly valuable.[15]

For example, one might consider a digital twin of an automobile. This digital twin would include simple, static data about the

---

[7] Sahal et al., *supra* note 4, at 19 (listing an example of digital twins of aircraft components); *see also* Jeffrey David Iqbal et al., *The Use and Ethics of Digital Twins in Medicine*, 50 J.L. MED. & ETHICS 583, 584 (2022) (mentioning engineering fields using digital twins including their use with power grids).

[8] While the concept of digital twins was first introduced by David Gelernter in 1991 in his book *Mirror Worlds*, "the core idea of using a digital twin as a means of studying a physical object" was pioneered by NASA in the 1960s. *What is a Digital Twin?*, *supra* note 2.

[9] *Id.*

[10] *See* Michael Grieves, *Virtually Intelligent Product Systems: Digital and Physical Twins*, *in* COMPLEX SYSTEMS ENGINEERING: THEORY AND PRACTICE 175, 175–200 (Am. Inst. of Aeronautics & Astronautics 2019).

[11] *What is a Digital Twin?*, *supra* note 2.

[12] Iqbal et al., *supra* note 7, at 584.

[13] *See* Attaran & Celik, *supra* note 3.

[14] Iqbal et al., *supra* note 7, at 584.

[15] *Id*.

automobile, such as its make, model, color, number of seats, automatic versus manual transmission, dimensions, and a graphical rendering of the automobile itself. It would also produce more complex real-time streaming data about the current state of the automobile: its current speed, the direction the steering wheel is pointing, fluid levels, tire traction, cabin temperature, surrounding weather conditions—the list is nearly endless. The data produced by this digital twin could be used to predict the likelihood of a breakdown, the sobriety of the driver, intended destinations, and countless other metrics that automotive manufacturers and drivers alike would find valuable. The digital twin could be used to remotely perform vehicle inspections, diagnose problems, or create simulations that provide information on how the automobile would perform under experimental conditions. One can easily imagine such technology, with its affinity for proactive maintenance, having broad applications within the realm of preventative medicine.

Digital twins within the medical space have the potential to facilitate more efficient and meaningful use of the providers' time and more agency on the patients' side. A digital twin within the healthcare context is like a living, digital patient replication.[16] As a parallel, a patient's digital twin—encrypted and hosted on a healthcare center's cloud server[17]—would contain their medical history, digital reconstructions of organs, demographics, and lifestyle data over the course of time.[18] What makes this model "living" is its ability to update itself based on its real-life counterpart through "various technologies such as sensors, high-speed communication, cloud computing, artificial intelligence," and more.[19] At this time, digital twin technology is expensive to the point of inaccessibility to the average American medical patient.[20] But as with other burgeoning technologies—take computers for example—production and maintenance costs will improve, making the

[16] Popa et al., *supra* note 5, at 1.

[17] Patrizio Armeni et al., *Digital Twins in Healthcare: Is It the Beginning of a New Era of Evidence-Based Medicine? A Critical Review*, 12 J. PERS. MED. (2022).

[18] Popa et al. *supra* note 5, at 2.

[19] *Id.*

[20] Armeni et al., *supra* note 17.

technology more efficient and cheaper. A computer that once took up an entire room now fits comfortably in the pocket of the average American consumer.

The list of benefits from incorporating such an extensive and, consequently, invasive tool into the healthcare system is vast. Some believe it could shift medical attention from predominantly treatment-based work to preventative care by having a fuller picture of what is happening within each patient's body.[21] This capability and the potential ease with which healthcare providers could perform digital consultations both prevents the loss of the diagnostic advantages of in-person visits and frees up healthcare providers' time for patients ready for specific and more urgent care.[22] From a systematic perspective, there is a possibility of cost reduction for patients and medical teams alike without the need for repeat tests for lost or forgotten information or for in-person regular health maintenance.[23]

Medical digital twins, though not yet widely used, have achieved initial success in application in areas including cardiovascular disease, orthopedics, surgery, and pharmacy.[24] An exemplary use case is a 2017 study that developed a non-invasive diagnostic test using digital twins.[25] The test aided healthcare providers in assessing the impact of vascular blockages on blood flow to the heart by combining the information of computed tomography ("CT") scans, artificial intelligence, cloud computing, and computational physiology.[26] In 2021, a digital twin was created to model the entire blood circulatory system that could be calibrated based on individual patients.[27] In 2022, a digital twin utilizing 3D X-rays simulated bone healing, allowing researchers to assess the risk of recurrent fracture under maximum weight loads while walking.[28] The anticipated leap from testing digital twins' capabilities in

---

[21] Popa et al., *supra* note 5, at 10–12.
[22] *Id.*
[23] *See id*. (listing cost reduction as a benefit of digital twins in healthcare).
[24] Sun et al., *supra* note 1, at 8.
[25] *Id.*
[26] *Id.*
[27] *Id.*
[28] *Id.*

medicine, to building a system in which modeling patients' bodies through digital twins is widespread and accessible, would give healthcare providers the ability to apply a wide range of scenarios to individuals' digital twins. These future uses of digital twins serve the purposes of precise, minimally invasive diagnosis and preventative care.

The data required to create a digital twin is expansive, detailed, and deeply personal. The future vision of medical digital twins in practice is that each individual would have their own "full-lifecycle [digital twin] body."[29] The digital twin would be created in a hospital at the time of birth from a collection of data gathered by healthcare providers pertaining to the body and health of the newborn.[30] This digital twin would grow and develop along with the child, serving as a life-long health record updated through wearable health trackers and routine checkups, and would operate as a means for providers to perform diagnoses and experiments throughout the individual's life.[31] The digital twin contains virtual models of the individual's internal organs, tissues, cells, or micro-environments that would constantly adjust to reflect the current state and health of the individual.[32] For the collection of such detailed and real-time biometric data, some envision a small chip or ingestible sensor, which as technology improves, would become smaller and smaller and, thus, less and less invasive.[33]

Equally important to note are the risks to privacy and related misuse or abuse of data associated with consolidating substantial intimate data about a patient. Depending on who obtains access to a patient's digital twin, there is an enormous risk for discrimination based on genetics, unseen conditions, or physical quirks that have the potential to affect insurance, employment, or other aspects of a person's livelihood.[34] The more people with access—technicians,

---

[29] *Id.*
[30] *Id.*
[31] *Id.*
[32] *Id.*
[33] Popa et al., *supra* note 5, at 10.
[34] *Id.* at 14; *see generally* Ifeoma Ajunwa et al., *Health and Big Data: An Ethical Framework for Health Information Collection by Corporate Wellness Programs*,

nurses, doctors, and administrative staff at different hospitals, or the staff of a third party data-hosting service, for example—the higher the likelihood of a data breach. With the extent of genetic material available, if digital twins become widely used in American healthcare systems and data falls into unethical hands, there is the potential for society to segment out portions of the population based on genetic disposition for survival or health.[35]

B. The Prevalence of Medical Data Breaches and the Implications for Patients

Though no industry is safe from data breaches, digital twins are poised to accelerate healthcare's already poor performance as one of the top targets for hackers desiring valuable data to sell on the black market.[36] Unlike other precious data, such as credit card information, healthcare fraud often takes longer to be discovered, allowing the stolen information to be used falsely for longer.[37] Over the past fourteen years, there have been a rising number of reported data breaches from the U.S. Department of Health and Human Services' Office for Civil Rights ("OCR"), stemming most frequently from hackers or information technology ("IT") incidents.[38] According to a report from the Health Insurance Portability and Accountability Act ("HIPAA"), almost 400 million medical records have been compromised since 2009, with three of the top ten breaches occurring in 2023.[39] As this number represents HIPAA violations, it shows only a portion of existing breaches. The rate of class actions against medical data breaches is also increasing,

---

44 J.L. MED. & ETHICS 474, 478 (2016) (discussing the use of digital twins in employer wellness programs).

[35] Popa et al., *supra* note 5.

[36] Skye Witley & Christopher Brown, *Health Data Breach Class Actions Surge as Cyberattacks Climb*, BL (Aug. 23, 2023, 5:00 PM), https://news.bloomberglaw.com/privacy-and-data-security/health-data-breach-lawsuits-surge-as-cyberattacks-keep-climbing [https://perma.cc/YL5F-SWXL].

[37] Rebecca Murray-Watson, *Healthcare Data Breach Statistics*, HIPAA J., https://www.hipaajournal.com/healthcare-data-breach-statistics/ [https://perma.cc/HCT4-KY7G] (last updated Sept. 19, 2023).

[38] *Id*.

[39] *Id*.

with the 2023 monthly average of class action lawsuits regarding medical data breaches nearly doubling the rate from 2022.[40]

Any data breach is a violation, but the effects of a medical data breach with an individual's genetic information and extensive medical history—all of which would be contained in a medical digital twin—increases the potential for abuse of the information. For example, many states have already begun criminalizing medical procedures, such as reproductive healthcare and gender-affirming care, in recent years.[41] Since the U.S. Supreme Court's 2022 decision in *Dobbs v. Jackson Women's Health Organization*,[42] in which it declared the previously protected right to abortion unconstitutional,[43] fourteen states have passed full bans on abortion, with an additional seven shortening the gestational limit.[44] Three states have criminalized self-managed (outside of a healthcare setting) abortion.[45]

Similar legal invasions of medical treatment have befallen gender-affirming care, or "age-appropriate care that is medically necessary" for many transgender and non-binary people who experience gender dysphoria, or distress from one's gender identity not matching their sex assigned at birth.[46] In recent years, legislatures across the country have ignored the American Medical Establishment's recommendations by introducing hundreds of bills

---

[40] Witley & Brown, *supra* note 36.

[41] *See generally After Roe Fell: Abortion Laws by State*, CTR. FOR REPRODUCTIVE RTS., https://reproductiverights.org/maps/abortion-laws-by-state/ [https://perma.cc/22PD-NAFV] (last visited Nov. 22, 2023) (mapping all current abortion bans and restrictions by state); *Map: Attacks on Gender Affirming Care by State*, HUM. RTS. CAMPAIGN (last updated Sept. 5, 2023), https://www.hrc.org/resources/attacks-on-gender-affirming-care-by-state-map [https://perma.cc/GS8X-6ZJ2] (mapping all laws or policies banning gender affirming care by state).

[42] Dobbs v. Jackson Women's Health Org., 142 S. Ct. 2228 (2022).

[43] *Id.*

[44] *Tracking Abortion Bans Across the Country*, N.Y. TIMES (last updated Oct. 7, 2023, 9:15 PM), https://www.nytimes.com/interactive/2022/us/abortion-laws-roe-v-wade.html [https://perma.cc/QRC2-QT4V].

[45] LAURA HUSS ET AL., IF/WHEN/HOW, SELF-CARE, CRIMINALIZED: AUGUST 2022 PRELIMINARY FINDINGS 1 (2022).

[46] *Map: Attacks on Gender Affirming Care by State*, *supra* note 41.

targeting access to gender-affirming care for people under eighteen, with twenty-two states passing laws or policy bans.[47]

C. Current State of Regulation for Data Privacy in Healthcare

Medical digital twins have yet to experience much litigation or regulation, but the adjacent topic of the healthcare industry's data privacy in the American regulatory scheme has consisted of flexible implementation and often ineffective and unsuccessful causes of action for victims of medical data breaches. The most significant pieces of legislation to date are the aforementioned HIPAA of 1996, which created "minimum protections and security procedures for the transfer of patient health information," and the Genetic Information Nondiscrimination Act of 2008 ("GINA"), which aimed to bar discrimination based on genetic information regarding insurance and employment.[48] 2010's Affordable Care Act ("ACA") ensured protection from data-based discrimination for individuals or families with prior conditions by forbidding insurance companies from precluding them from buying private health insurance at all.[49] Most statutes, even if prescriptive, like HIPAA, use a regulatory approach that enforces "broad regulations designed to promote internal organizational cybersecurity management" and allows organizations substantial flexibility in determining how, when, and which cybersecurity requirements they implement.[50]

Once a data breach occurs, courts have been unclear on whether patients exposed to data breaches have suffered harm sufficient enough to bring a claim in the first place.[51] This uncertainty stems from the fact that the immediate "harm" relating to data breaches usually comes in the form of threatened future harm.[52] Consider a

---

[47] *Id.*

[48] Terry Wong, *Characterizing the Harms of Compromised Genetic Information for Article III Standing in Data Breach Litigation*, 53 COLUM. J.L. & SOC. PROBS. 461, 470 (2020).

[49] Ifeoma Ajunwa, *Genetic Data and Civil Rights*, 51 HARV. C.R.-C.L. L. REV. 76, 88 (2016).

[50] Charlotte A. Tschider, *Locking Down "Reasonable" Cybersecurity Duty*, 41 YALE L. & POL'Y REV. 75, 120 (2023).

[51] Witley & Brown, *supra* note 36.

[52] Daniel Bugni, *Standing Together: An Analysis of the Injury Requirement in Data Breach Class Actions*, 52 GONZ. L. REV. 59, 76 (2017).

similar situation in which one's credit card is stolen: the "harm" of a hacker immediately spending money with that stolen information is clear. Medical data breaches resemble a hacker stealing a credit card and then waiting months to spend anything, with no opportunities to cancel the card to prevent its misuse. If the card owner had to wait to bring a claim until money was spent, it is possible that the months in between the card theft and the actual harm of the money spent would be great enough to make the credit card thief hard to trace.

In the case of a digital twin, waiting for the "harm" to occur—exposure of one's complete medical profile and its implications—is untenable, as no court-ruled damages can fix a privacy violation like it can return stolen funds. Since there is no quick or easy remedy to this degree of harm, there would be long-term effects: from potential stigma for a predisposition, to a serious illness or legal troubles from evidence of a criminalized medical procedure.

The courts' vague stance on healthcare data breach victims' right to recovery paired with the soft regulations of healthcare data have created a space for breaches to propagate like viruses, with injured parties left with few resources for justice.

III. INEFFICACY OF CURRENT LAW ON DIGITAL TWINS IN HEALTHCARE

The retroactive nature of the American legal system is understood and considered to be standard at this point, but as experts predict the potential pitfalls of burgeoning technologies, many believe that early regulation will help build the framework necessary for digital twins to work effectively in healthcare.[53] Numerous technological advances have emerged unexpectedly without much time to prepare a societal foundation. But as industry leaders can anticipate approaching technologies, there is a desire to establish and modify regulatory schemes while the technology is malleable and has yet to cement its impact on society.[54] Once a data breach

[53] Angira Sharma et al., *Digital Twins: State of the Art Theory and Practice, Challenges, and Open Research Questions*, J. INDUS. INFO. INTEGRATION, Nov. 2022, at 12.

[54] Popa et al., *supra* note 5, at 3.

occurs, recovery is difficult, as there is not a clear cause of action for plaintiffs to utilize successfully.[55]

The most common routes attempted by plaintiffs are claims under tort, contract, or property law, but all fall short in varying degrees. Tort law is most often utilized through claims of negligence, breach of contract, unjust enrichment, amongst others. Although more successful than other areas of common law, plaintiffs frequently struggle to convert the traditional causes of action to fit the recent and developing space of medical cybersecurity.[56] Most complications under tort claims arise in proving a negligence case, most notably proving causation and damages.[57] Proving proximate cause means showing that the risk of injury was not in reasonable foresight of the defendant.[58] Damages prove difficult to claim for "wrongful disclosure of genetic information" as the harm from this kind of leak can exceed monetary loss, which courts are often reluctant to remedy.[59]

Contract and property law are even less effective in delivering data breach plaintiffs with a cause of action.[60] Bringing a contract claim against the "primary malicious actor" is near impossible when that actor is an anonymous hacker.[61] Under property law, the absence of physical property deprivation bars a successful action.[62] Though intellectual property law may get closer to data breaches conceptually, there are no current property rights associated with

---

[55] *See generally* Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737 (2018) (examining why courts have struggled to conceptualize harms caused by data breaches).

[56] Wong, *supra* note 48, at 472.

[57] Ifeoma Ajunwa, *Genetic Testing Meets Big Data: Tort and Contract Law Issues*, 75 OHIO ST. L.J. 1225, 1253 (2014).

[58] *Id.*

[59] *Id.* A major complication in proving causation and damages is that plaintiffs have not yet suffered any harm. In turn, plaintiffs argue that they have suffered harm "in the form of a future risk of injury," which courts are inconsistent in recognizing as a cognizable harm. Daniel J. Solove & Danielle Keats Citron, *Privacy Harms*, 102 B.U. L. REV. 793, 817 (2022).

[60] Wong, *supra* note 48, at 473–74.

[61] *Id.* at 473.

[62] *Id*. at 474.

one's personally identifiable health information ("PII") that would allow them to control use or distribution of that information.[63]

This already inadequate legal footing for actions in healthcare data breaches stands ready to rapidly worsen. Digital twins are only just entering the realm of healthcare, and when they fully integrate into medical systems, healthcare has the potential to look markedly different than it does now. As a society it is often impossible to keep up with the runaway train of technology. However, in some cases—like when implementing a technology, for which there is already an understanding, into a new sector—there are enough sightlines into the future to enable collective work. Legislatures, courts, and industry experts alike can draw a framework through which the new technology can grow and operate safely. The solution begins with looking at the cybersecurity and privacy implications of current digitization in medicine and locating areas of improvement both for prevention of harm and remedying harm when a breach happens. Lawmakers should work alongside medical digital twin experts to require the most protective standards for this sensitive data and ownership rights for the patients who produce and should own that information. It is possible to set regulatory requirements preventing healthcare providers from handling data negligently instead of only trying to pick up broken pieces in the runaway train's wake.

IV. IMPORTANCE OF PATIENT AGENCY IN DATA PRIVACY

It is essential to give patients agency over general access to their digital twin and a clear cause of action for recovery. This agency has impact both in terms of envisioning the safest framework for using digital twins in healthcare and for creating proper avenues of recovery for those who inevitably fall victim to data leaks. Digital twins have only been sampled in a limited number of specific areas of medical practice, but as the industry looks to the future, many have argued that the best way to remedy privacy threats to patient information is to make sure that data ownership remains in the patient's hands. Here, the suggested solution is that data use access

[63] *Id.* at 473–74.

is granted only by the patient and that legislative bodies work to enshrine and protect these principles.[64]

A better understanding of patient agency in relation to digital twins proceeds with an examination of what it means for a patient to own their digital twin, discusses ways to mitigate threats to digital twin data, and finally, considers patient agency through the presence of a successful cause of action.

A. Defining Data Ownership

One primary question remains unanswered: what does patient agency look like in practice and what does it mean to "own" one's data? Patient agency must address control over the use of the data and not the patient's direct possession of the data. While a patient's ownership of their data is essential to the protection of their privacy, it is hardly reasonable to expect the average patient to possess the computer systems and database administration skills necessary to maintain their own digital twin data, on, for example, their laptop or desktop computer. Issues would also arise as to the consistency of the data retained by each patient and the data used by healthcare providers. Differing data formats and transfer protocols would add insurmountable complexity to the effective transfer of data to the provider and interpretation of the data by the provider.

The data formats and processes involved with digital twin technology are extremely complex, even by the standards of a data professional. Low universality—or the ability to use the data across a wide variety of systems and applications—of digital twin data is the dominant obstacle slowing the proliferation of digital twin applications.[65] The transfer and use of digital twin data across scenarios, such as the transfer between artificial intelligence software and visualization software, is confounded by differing requirements and constraints that each scenario imposes on the

---

[64] Skander Tahar Mulder et al., *Dynamic Digital Twin: Diagnosis, Treatment, Prediction, and Prevention of Disease During the Life Course*, 24 J. MED. INTERNET RSCH. 1, 7 (2022).

[65] Meng Zhang et al., *Digital Twin Data: Methods and Key Technologies [Version 2; Peer Review: 4 Approved]*, DIGIT. TWIN (2022), https://digitaltwin1.org/articles/1-2 [https://perma.cc/33VM-ZZ8V].

format of the data being transferred.[66] The exchange and parsing of data between applications is further complicated by factors like the physical sensor producing the data (e.g., subdermal, ingestible, or wearable sensors), the interfaces that allow interaction with the data by humans, and the communication protocols that send the data over networks, like the internet, between applications.[67] As variation in any one of these dimensions would cause disruptions in the effective use of a patient's digital twin, it would be unreasonable to put the onus of data format and maintenance on the patient.

Adding to these integration complications is the potential for patients to lose their data or not maintain appropriate backups. Due to the risks in consistency and usability of the data, the costs of maintaining data storage and backups, and the skill gaps between the average patient and a database administrator qualified to maintain this type of data, it becomes more reasonable to delegate the hosting and retention of patient digital twin data to hospital or public health data centers, while the patient's ownership of the data manifests as ownership of the access to their data. While the current medical record model points to greater feasibility for health centers to store data, the privacy risks make this option untenable.

The notion of a patient's agency over the use of their data by an approved healthcare provider has an additional, indirect challenge: the patient's approval of their data's use in wider analyses. A patient's digital twin, when taken in context with other patients' digital twins, could be used for any number of tangential applications, such as the training of artificial intelligence and machine learning models, analysis of demographic or population health, or mass public health simulations. In 2020, researchers created population simulations modeling the spread of COVID-19 using digital twin technology,[68] and with the approach of more detailed and personal digital twins, advanced simulations like this will become increasingly prevalent. Patients should be able to consent to the involvement of their digital twin data in such

[66] *Id.*
[67] *Id.*
[68] Sun et al., *supra* note 1, at 10.

simulations and population studies, along with other types of tangential analyses that may seek to make use of their digital twin.

B. Mitigation of Data Privacy Threats

To remedy threats to a patient's data privacy within the proposed patient-owned-data-access model, two requirements of the data storage system must be held: (1) the system must ensure that every data transaction is carried out only with the express consent of the patient; and (2) the system must provide the patient with the ability to selectively disclose only the data they deem necessary for a given analysis.[69]

Blockchain technology has the potential to implement the above delineation of patient agency over which data is shared and when. A blockchain, or distributed ledger, can be thought of as a log of ordered transactions between entities that do not trust one another.[70] The security of blockchain transactions comes in the form of its distribution: all parties participating in the blockchain have replicas of the ledger and, therefore, are able to create consensus for which transactions are legitimate and verify the order in which transactions happen.[71] If a healthcare provider needed access to a patient's digital twin, their request would create a transaction on the blockchain, requiring the patient to provide a signature via their private key, a secure "password" of letters and numbers that only the patient possesses and accesses.[72] Transactions for which the patient has not provided their private key would be invalid, the request for data would not be completed, and the first requirement of the data system, a patient's consent to access their data, would be fulfilled.[73] To meet the second requirement, the range of data to be accessed must be included within the data request and the resulting

---

[69] Sadman Sakib Akash & Sadek Ferdous, *A Blockchain Based System for Healthcare Digital Twin*, 10 IEEE ACCESS 50523, 50532 (2022).

[70] Tien Tuan Anh Dinh et al., *Untangling Blockchain: A Data Processing View of Blockchain Systems*, 30 IEEE TRANSACTIONS ON KNOWLEDGE & DATA ENG'G 1366, 1366 (2018).

[71] *Id.*

[72] Akash & Ferdous, *supra* note 69, at 50542.

[73] *Id.* at 50532.

transaction.[74] The range could be provided either by the healthcare provider issuing the request to be approved by the patient, or it could be specified by the patient at the time of their provision of the private key. This would ensure not only the patient's control of access to their data but also the composite segments of data sets that create their digital twin's components. This same paradigm would apply to any request by a healthcare provider to alter or delete any part of a patient's digital twin data.

In addition to a patient's consent to access their data, legislation must address the duration of a third-party's access to patient information.[75] There exists an ethical question surrounding the continual use of one's digital twin data. Digital twins in current industry settings collect both historical and real-time data about their physical counterparts, and in a medical application, digital twins would do the same for patients.[76] While continuous monitoring of a patient's digital twin would lead to vast increases in the ability to detect and track progressive disease risk, the consent of the patient must be explicitly granted, and the patient must be fully informed with all ethical conditions specified.[77] Conceivably, duration of access and revocation thereof would be enforced and verified by the blockchain, but current industry standard database access logs would also be a viable option. Having duration managed by the blockchain would be ideal, as access could be revoked automatically after a set period or at the end of a particular course of treatment.

A possible challenge to patient agency over healthcare data use can be found in current practices. One might say that this level of control of the patient over their data, maintaining the onus of granting or shielding access to their personal data, is overly protective and unnecessary. Current healthcare systems and financial institutions alike retain ownership over vast amounts of deeply personal and confidential data about their clients, and while these clients have the right to access and distribute this data at-will, they are not burdened with the task of ensuring the security of the

---

[74] *Id.*
[75] Sahal et al., *supra* note 4, at 32.
[76] *Id.* at 16.
[77] *Id*. at 32.

data that pertains to themselves. One could even argue that existing patient confidentiality laws and HIPAA would guarantee the confidentiality of one's digital twin data. With patient advocacy and data encryption, healthcare-based servers could host a patient's data, and the patient would have the ability to use and grant access to that information. This concept is not dissimilar to having an apartment in an apartment building—the tenant controls access and use of the apartment but does not own the building. In this analogy, the regulatory process would protect the tenant's rights by requiring reasonable levels of maintenance and safeguards from the building owners.

While true that personal data is widely held by existing healthcare entities requiring no management on the side of the patient, there is no central repository of all health data pertaining to a particular patient, which is what the medical digital twin promises to provide. Given the centrality and sensitivity of the digital twin data, limiting the number of access points to the data greatly reduces the risk of access from unauthorized entities and bad actors; this is what the suggested framework seeks to provide. Furthermore, allowing even a trusted physician access to the entirety of one's digital twin could be perilous for the patient.

In the post-*Dobbs* era, laws regarding female reproductive health vary greatly between states, so the legitimate access to a patient's digital twin by a trusted provider could result in criminal charges to the patient if they are in a state that criminalizes abortion, and the digital twin contains evidence of the patient receiving one. Therefore, the patient's control, not only over general access to their digital twin, but also their control of granular access to specific data, is essential to protect the patient's privacy.

C. Patient Agency Through Proper Causes of Action

Amid the consistent breaches in medical data, class actions have been on the rise, but courts are split over what is required to deem a patient sufficiently "injured" by a medical data breach.[78] Regarding data breach class actions, most courts end up dismissing plaintiffs

[78] Daniel Bugni, *Standing Together: An Analysis of the Injury Requirement in Data Breach Class Actions*, 52 GONZ. L. REV. 59, 66 (2017).

for lack of standing.[79] The common themes among dismissed class actions include the "speculative nature of the harm" (in other words, the courts not considering theft of data harmful until something like active identity theft occurs), the "passage of time" after the data was breached, and the "sophistication" of the data thief (meaning data that was exposed through theft of property or another non-hacking method).[80]

Courts that have granted standing for medical breach class actions have either posed injury upon the initial breach before any identity theft commences, found the "injury-in-fact" to be the heightened risk of harm associated with the breach, or treated the disclosure of personal information as the injury.[81] In *Remijas v. Neiman Marcus*,[82] the Seventh Circuit held that the exposure of personal information was the injury itself when a hacker stole 350,000 credit card numbers from Neiman Marcus.[83] First, the court reasoned that requiring the plaintiffs to wait for the threatened financial crime added time which made identity theft harder to trace.[84] Second, there was no other reason for a hacker to steal credit card information besides to inflict identity theft or credit card fraud.[85] Additionally, the court held that information breaches require a "process of sorting things out," which has identifiable costs, and since these costs arise as soon as the breach occurs, the initial breach itself constituted the injury.[86] In *Krottner v. Starbucks Corp.*,[87] someone stole a laptop containing 97,000 unencrypted Starbucks employee names, addresses, and social security numbers.[88] Like the Seventh Circuit in *Remijas*, the Ninth Circuit found that the mere increased threat of future harm was enough to

---

[79] *Id.*
[80] *Id.* at 67–71.
[81] *Id.* at 76.
[82] Remijas v. Neiman Marcus Group, LLC, 794 F.3d 688 (7th Cir. 2015)
[83] *Id.* at 690, 693–94.
[84] *Id.* at 693.
[85] *Id.* ("Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities.").
[86] *Id.* at 692.
[87] Krottner v. Starbucks Corp., 628 F.3d 1139 (9th Cir. 2010).
[88] *Id.* at 1140.

establish standing.[89] In *In re Sony Gaming Networks & Customer Data Security Breach Litigation*,[90] hackers breached Sony's online gaming network, accessing millions of customers' home and email addresses and credit and debit card information.[91] Like the previous cases, the court found that the wrongful disclosure of sensitive information itself constituted the harm.[92]

By taking the minority of courts' lead and leaning towards precedents finding standing for class actions regarding data breaches, policy should allow for both class action and individual causes of action when the preemptive protective systems fail. Whether the exposure of current medical records counts as enough "harm" according to the American legal system is irrelevant when one considers the *degree* of livelihood-ruining information available when a patient's digital twin is illegally accessed. With today's explosive market for data, and countless internet actors from individuals to conglomerates alike waiting to buy or access it, as soon as a breach of such valuable information has occurred, level of harm should easily be established for the sake of standing, as there is no way to close that Pandora's box.

V. REGULATORY STAKES AND DIRECTION FOR THE FUTURE

Unlike some similarly disruptive industry innovations of the past, medical professionals, technology experts, and legislative bodies have the advantageous opportunity to work together to design, regulate, and ensure the implementation of safe data practices while digital twin technology is developed.[93] With the current frequency of medical data breaches in the United States and the additional harm that hacking into not only one's medical records but essentially one's genetic and personal makeup, the *post facto* effect of legislative policy's characteristically lagging nature comes up too little, too late.[94] As technologies emerge, they are generally

---

[89] *Id.* at 1143.

[90] *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942 (S.D. Cal. 2014).

[91] *Id.* at 954–55.

[92] *Id.* at 961–62.

[93] Popa et al., *supra* note 5, at 19.

[94] *Id.*

seen to be more malleable or easy to modify before they are established within the threads of society, making now the ultimate time for lawmakers to recognize and act on the importance of upholding data security for digital twins.[95]

A. Importance of Proactive Regulation Against Harm

A person's genes are often viewed as a clear map of their physical personhood, but with the wrongful disclosure of such "clear" information, comes a complicated web of consequences. Besides the immediate fears of employers finding reasons—intentionally or unintentionally—not to hire a person who may be prone to certain genetic diseases, or more egregiously, have DNA markers the employer finds distasteful, there is also the potential for genetic essentialism, genetic determinism, and genetic coercion.[96]

Genetic discrimination arises most frequently from the widely held sense of genetic essentialism, or rather, the "reductionist view of human beings as essentially consisting of their genes."[97] The idea that one's health and behavior are predetermined by their genetics and that their personal traits are "predictable and permanent, determined at conception, [and] 'hard-wired' " into an individual—called genetic determinism—creates an overreliance on genetic information, turning probability of a disease into inevitability.[98]

Genetic coercion puts genetic essentialism and determinism into action, as the "economic, social, and moral compulsion to scrutinize and police the genome."[99] The economic compulsion arises from the lack of universal healthcare in the U.S., making life with medical conditions financially difficult. The social compulsions conceivably come from the desire for nonconforming genes to be exposed.[100] The concept of a moral compulsion for genetic coercion is the idea that it is one's duty to prevent deleterious genetic mutations from being passed down to future generations.[101]

---

[95] *Id.* at 3.
[96] Ajunwa, *supra* note 49, at 79.
[97] *Id.* at 80 (citation omitted).
[98] *Id.* at 81.
[99] *Id.* at 82.
[100] *Id.*
[101] *Id.* at 83.

Fostering this behavioral genetic reductionism could open the door to using genetics more ardently in the criminal justice system, moving beyond forensic identification and into areas like claiming predictions of recidivism or "evidence" of flight risk.[102] While it may seem easy to avoid these harmful mindsets, they developed naturally as genetic testing became more prevalent in society. With the enormous influx of access to one's genetic information with the emergence of medical digital twins, active steps are necessary to combat the further development of the human proclivity for discrimination.

Congress has recognized that with the presence of more individuals' genetic data comes "the potential misuse of genetic information to discriminate in health insurance and employment."[103] When given access to one's genetic information and possible insight into present or potential genetic conditions, American employers have a history of either denying or replacing employees found to have "genetic flaws."[104] Not only is one's livelihood possibly affected, but the actual management or treatment of one's genetic illness may also be in jeopardy.[105] As a country without universal healthcare, the U.S. leaves care for genetic conditions to one's individual or workplace insurance.[106] With a genetic condition exposed via the data breach of one's digital twin, insurance companies—though not able to deny coverage completely—can drastically increase rates on individual insurance. Even if an individual is lucky enough to retain their insurance through their employer, there is no legislation preventing insurance companies from hiking up premiums for employers with high-risk employees—a disincentive for hiring.[107] While the presence of GINA and elements of the ACA are meant to legally prevent this mistreatment, it does not prevent the exposure and probable harm of an illegal data breach: once information is uncovered, discriminatory bias can take

---

[102] Ellen Wright Clayton et al., *The Law of Genetic Privacy: Applications, Implications, and Limitations*, 6 J.L. & BIOSCI. 1, 22 (2019).
[103] Ajunwa, *supra* note 49, at 85.
[104] *Id.* at 87.
[105] *Id.*
[106] *Id.*
[107] *Id.* at 89.

root, creating potentially irreparable damage, especially without a direct cause of action.[108]

Though GINA prohibits health insurers and employers from discriminating against a person because of their genetic makeup, and the ACA prevents insurers from precluding those with prior conditions from having insurance, neither prohibit the use of genetic information from heath records in underwriting.[109] Directly regulating insurance underwriting practices becomes incredibly difficult as the insurance industry has been operating for centuries and is entangled in government expenditures such as Social Security Disability Insurance and aspects of Medicaid.[110] Instead, regulating the safety and use of individuals' digital twin data operates directly at the heart of the concern: protecting the genetic information and making the possibility of genetic discrimination less likely in the first place.

Combined with information from one's digital twin, it would be fairly easy to use unrelated points of data to craft the presumed story of an illegal abortion. The general genetic discrimination described above may take some time to become entrenched into the American zeitgeist, but as the criminalization of medical procedures in reproductive health and gender affirming care is on the rise, exposure of a person's digital twin data could have immediate and severe consequences. When the Court decided *Dobbs* in 2022, one of the initial fears in the reproductive health community was the exposure of data from menstruation tracking applications.[111] As states continue to criminalize abortions, law enforcement could use tracked menstruation data to prosecute people who appeared to be pregnant at one point and then seemed to suddenly no longer be pregnant, implying an abortion. With the implementation of digital twins in healthcare, those that could become pregnant might even be at risk of prosecution for medical situations that only look like

---

[108] *See id.* at 85 (going in depth into the GINA and comparing it to the ACA).

[109] Clayton et. al., *supra* note 102, at 25.

[110] *Id.*

[111] *See, e.g.*, Emilie Smith, *Cycle-Tracking Apps and Data Privacy in the Post-*Roe *Climate*, MARQ. UNIV. L. SCH. FAC. BLOG (Oct. 11, 2022), https://law.marquette.edu/facultyblog/2022/10/cycle-tracking-apps-and-data-privacy-in-the-post-roe-climate/ [https://perma.cc/32W9-G2NR].

illegal termination of a pregnancy.[112] Pregnancy loss can often look like a self-managed abortion.[113] If a person's digital twin detailed the early loss of a pregnancy and that person had at one point searched abortion online, or texted a friend about it, the two pieces of unrelated data could be cobbled together as "evidence" of an illegal abortion.[114] One's connection to the topic of abortion would not even need to be as direct as googling the word "abortion."

Drawing predictive arrows to people who can become pregnant is not a new or difficult task. Over a decade ago, the retailer Target was able to put together an analytical model that looked at shoppers' consumption habits to predict who would likely soon become pregnant, and with the growth in machine learning and predictive technologies, an actor could easily put together a similar model with similar, seemingly mundane data.[115]

A fair question is who would take the time and energy to frame someone for an illegal abortion, or even to hunt through someone's medical digital twin to find evidence of a legitimate one? Perhaps it seems far-fetched and fearmongering, but as abortion looks like healthcare to one person and murder to another, there is incentive for the energy spent. The actors most likely to meddle in medical data of others are law enforcement and nongovernmental "vigilantes," individuals who attempt to collect data to turn in to law enforcement, or to bring a civil suit under state laws that allow for direct claims against those helping facilitate an abortion under aiding and abetting provisions.[116] The data needed to bring such a suit is likely not difficult to find; under the relevant legal precedents, digital twins would be hacked and the data sold to data brokers. After *Dobbs*, two-dozen data brokers continued pursuing and marketing information about pregnant people, ignoring warnings from Democratic lawmakers.[117] The Center for Democracy and

---

[112] Anya E.R. Prince, *Reproductive Health Surveillance*, 64 B.C. L. REV. 1077, 1115 (2023).

[113] *Id.*

[114] *Id.*

[115] Aziz Z. Huq & Rebecca Wexler, *Digital Privacy for Reproductive Choice in the Post-Roe Era*, 98 N.Y.U. L. REV. 555, 586 (2023).

[116] *Id.* at 581–82.

[117] *Id.* at 582–83.

Technology found that law enforcement and intelligence agencies "spend millions on purchases of private-sector data from data brokers."[118]

It is also important to note that, as with many elements of the criminal justice system, people who already experience unjust targeting and profiling from racist and bigoted societal structures are and will be the main targets of these types of reproductive health witch hunts. In a study performed post-*Dobbs* by If/When/How, investigations into pregnancy terminations occurred in twenty-six states despite the far fewer number of states in which abortion is criminalized.[119] Out of the sixty-one cases in the investigation, the defendants were mainly people of color and lower income, and overzealous "police and prosecutors" used criminal laws not meant to apply to pregnancy termination, including murder and homicide in 43% of the studied cases.[120]

This same type of data abuse can occur relative to gender-affirming care. The recent wave of state legislative attacks on gender-affirming care for young people could lead to abuse of leaked medical digital twins. In states where gender-affirming care has been banned for people under the age of eighteen, transgender and non-binary youths and their supportive families have had to travel to other states to access the necessary healthcare.[121] Though states have not had much luck prosecuting illegal actions performed in states where that action is legal, in a new landscape of medical digital twins, a data leak containing the presence of gender-affirming healthcare information may be subject to such prosecution. The consequences of such accusations are already looking dire with threats to take children away from parents supporting them in their transition, which could have a chilling effect both on families that want to be supportive and on the youths themselves, preventing what is sometimes life-saving care.[122]

---

[118] *Id.*

[119] HUSS ET AL., *supra* note 45, at 2.

[120] *Id.* at 4.

[121] Adam Schwartz, *Trans Youths Need Data Sanctuary*, ELEC. FRONTIER FOUND. (Aug. 26, 2022), https://www.eff.org/deeplinks/2022/08/trans-youths-need-data-sanctuary [https://perma.cc/EQ9D-62LJ].

[122] *Id.*

B. Potential Proactive Policy

Going beyond a retroactive lens, policymakers will benefit most from collaborating and supporting the researched solutions for data security and patient agency surrounding digital twins through regulating healthcare systems' data privacy protection practices in maintenance, monitoring, and access points.[123] According to research presented by the HIPAA Journal, the most effective way for healthcare systems to prevent data breaches is to encrypt the information, essentially making it unreadable to anyone who does not have the encryption key—the owner of that key being the owner of the digital twin: the patient.[124] To protect the encryption key, steps like two-factor authentication and multi-walled password systems allow for designated data monitors to register a breach threat and lock down access before the hacker retrieves a digital twin's information.[125]

Hospitals and healthcare providers will incur additional costs to implement higher requirements of data security through staffing and maintenance, and this poses a potential threat to consumers in the way of increased fees. While this might increase the overhead for healthcare practices, it is nonetheless a meaningful investment that will be rewarding in the long run and will further protect healthcare centers from data breach liability. Where policy has a chance to shine is through the preventative codification of secure data practice structures and their required maintenance by hospitals and healthcare systems. This is opposed to symptom-specific regulations that prevent certain entities from taking advantage of the leaked data. Not only is this retroactive legislation underinclusive, but as it occurs after the harms have carved their place into the infrastructure of digital twins in medicine, any necessary systemic changes will likely be clunky or even infeasible. Creating a regulatory framework in which medical digital twins can develop might look like specifying qualifications for where this highly sensitive information can be stored (i.e., special healthcare facility servers). There might

---

[123] *See* Sahal et al., *supra* note 4, at 16 (detailing requirements for building a system with digital twins in healthcare).

[124] Murray-Watson, *supra* note 37.

[125] *See id.* (mentioning the importance of registering threats ahead of a breach).

also be requirements for encrypting the digital twin before it is sent to a cloud server, along with reasonable monitoring and maintenance schemes that would allow for breach detection in time to prevent a hacker from acquiring full access. Legislation should also protect the patient's role by deferring to them in questions of access and by allowing for successful causes of action through acknowledging harm at the point of the data breach. Ultimately, the harm of having one's medical digital twin leaked or sold to a bad actor should be viewed as detrimental, and the preclusion of such should, therefore, fall under the duty of healthcare systems to protect and the duty of legal systems to enforce.

C. Preventing Entrenched Harm Outweighs Legal Overbreadth and Technological Restriction

While the usual *post facto* nature of legislation often leaves the law lagging behind technological advancements, those opposed to preemptive legislation could argue that a reactive posture is necessary to ensure regulations are tailored narrowly enough to effectively regulate the technology in question. When laws are created to proactively regulate a budding technology, like medical digital twins, the risk is that preemptive law becomes uninformed law. The preemptive regulation, as proposed by this Article, could, in practice, be either overbroad and unenforceable or too restrictive and, thus, hinder innovation within the technology it hopes to make successful. However, waiting for case law to address the individual harms caused by medical digital twin data breaches or until a large enough harm occurs for legislative bodies to act, allows the healthcare industry to establish and entrench its digital twin practices. In following this path, the development of regulations surrounding medical digital twins will mirror the current issues facing data security in healthcare: confusion over successful claims and a lack of infrastructure in need of a digital overhaul to fix.

As discussed in previous sections,[126] the U.S.' current data security regulations are inadequate for dealing with data breaches in healthcare, and once digital twins are integrated into the medical field, the consequences will be more severe.

---

[126] *See supra* Part III.

VI. CONCLUSION

The potential of digital twins' use within the medical domain creates the need for major shifts within our data privacy and security legal paradigm. With the increased sensitivity and breadth of data captured by a digital twin, patients must be able to rest assured that their data is private, protected, and confidential. Further, patients must be provided with a legal means of recovery to hold accountable any institutions found responsible for data leaks and breaches in confidentiality.

To assure patients of the security and confidentiality of their digital twin, one solution would be to shift the ownership of a patient's personal health information away from healthcare providers or other third parties and allow patients the ability to own and control access to their own sensitive data. An implementation of this type of ownership could be realized using blockchain technology and data encryption. Data access requests from healthcare providers would register as blockchain transactions that can only be approved by the patient via the provision of a private key, and a patient-controlled encryption key would enforce this. The patient must also be able to control which segments of data a healthcare provider has access to for a given application and the duration over which access is granted. The goal is to limit the points of access to an individual's medical digital twin so that the patient has agency and understanding as to who is accessing the information and when.

Beyond these foundational steps, some of which this Article addresses, there is a myriad of consequences to breached data security that must be addressed in legislation. Genetic discrimination limits job opportunities or treatment at those jobs because, despite prohibitive legislation, humans will always have biases and will find ways to live and work by them. Underwriting affected by genetic determinism could make healthcare financially unfeasible based on genetic predispositions that are mere suggestions relied on as determined fact. Criminalization of medical care in spaces like reproductive health and gender-affirming care stand to ruin the lives of those whose digital twins are leaked and

used as evidence against them, along with the lives of family members and medical professionals who worked to support them.

The current approach of the American legal system in handling medical data breaches will prove increasingly inadequate as the higher value of a digital twin's information (due to its breadth and depth) will further entice hackers. The resulting damage will evolve from potential individual harm to more profound societal repercussions, including genetic discrimination. Working off prior medical data breaches and with industry leaders in the use of digital twins in healthcare, policymakers' best option is to create the safest environment possible for this new technology to emerge, by holding the healthcare industry accountable for protecting Americans' most intimate medical information. Regulations must create the structural framework that will provide medical digital twins with the infrastructure to secure personal data as well as a program to relentlessly monitor for bad actors trying to breach that security.

No system, regardless of how well-planned, is free of flaws or areas where mistakes or bad actors can slip through the cracks. Because of this, part of the efforts to enable a successful transition into the age of medical digital twins should be a legal path of remedy for when the system fails. A presumption of harm at the onset of the breach and legislation creating a private cause of action would work in this direction. The stakes are high. Lawmakers should hold in the balance people's ability to work, care for their families, remain free of unjust prosecution, and retain control of their health, safety, and privacy. The upfront work may seem daunting, but the efforts of collaboration among lawmakers and medical technology experts to create a sound foundation for the future of medicine pales in comparison to the tragic mess awaiting a system left to develop under a "wait and see" strategy.