Texas Public Policy Foundation

FROM CLIPBOARD TO CLOUD:

Ensuring Patient Privacy and Portability in Health Records

WRITTEN BY **Brooke Garner and Charlie Glover**

AUGUST 2026

KEY POINTS

- HIPAA protects institutions, not information. Once health data leaves a covered entity for an app, vendor, or broker, federal protection ends, and Texas law leaves that gap open.
- The interest at stake is not only access to clinical records. It is control over all health data, including wearables, apps, and genetic tests, that now moves unprotected through the commercial market.
- Texas has repeatedly affirmed patients' right to their records, yet that right lapses the moment data crosses the institutional line into the unregulated commercial sphere.
- The harm is real and documented. Health apps have sold patient data to advertisers, brokers have exposed clinic visits through location data, and bankruptcies have put sensitive genetic records up for sale.

INTRODUCTION

Few possessions are more personal than one's own medical history, and few are harder to actually hold. Texans' right to their health records has been repeatedly affirmed through actions taken by the state, yet they continue to be faced with a litany of barriers such as portals, delays, and an overall lack of transparency that keep those records just out of reach. A national study found that in 2017-2018, about 54% of U.S. adults reported having even been offered online access to their records, and among those who were, only about 57% reported actually accessing them—meaning only roughly three in ten adults actually accessed their records (Trivedi et al., 2021). A right that a patient cannot legitimately exercise is, in practice, not much of a right at all. Moreover, even this familiar right captures only a fraction of the problem: the greater failure lies not in whether patients can reach the records held for them inside the clinic, but in how little control the individual retains over the far larger body of health information about them that now moves, unprotected, through the commercial world beyond it.

The through-line of the analysis that follows is that protection in this domain attaches to the institution, not the information: the moment data leaves the doctor's office, the patient loses both sight of it and any say over it. Texas therefore has a distinct interest in protecting the individual ability to reassert ownership of, and control over, one's own health data. The existing legal framework is not built to do so. Federal law only reaches a narrow

continued

set of "covered" institutions under HIPAA, and Texas' own landmark data privacy and security statute expressly exempts them, leaving a gap precisely where the data, and the harm, now travels (45 CFR Section 160.103; Business and Commerce Code Section 541.002).

This paper ultimately argues that the consumer protections Texas already secures under the Texas Data Privacy and Security Act—the so-called "Texas Digital Bill of Rights"—should be extended into the health data context to guarantee verifiable control and portability, affirmative individual consent over the use and sale of health information, and clear parental rights over children's records (Dunmoyer & Whiting, 2022; Business and Commerce Code Section 541.051). The recommendations developed below also confront this coverage gap directly: by adopting the broader definition of "covered entity" found in the Texas Medical Records Privacy Act (Health and Safety Code Section 181.001), and by requiring that consent and auditability follow health data once it leaves an institution, so that protection attaches to the information itself rather than to the office that first held it.

BACKGROUND

This paper's argument rests on a premise and a distinction that this section establishes before the analysis proper begins: that access to one's health information is a settled legal right, and that the data over which an individual interest is vested extends far beyond the clinical record to which the law's protections are principally tied.

The right itself, however, is neither novel nor broadly contested. Texas has affirmed it repeatedly and deliberately. The Texas Medical Records Privacy Act (TMRPA) obligates a provider using an electronic records system to furnish a patient's electronic health record, on written request, no later than the 15th business day (Health and Safety Code Section 181.102), and the Texas Medical Board independently requires physicians to produce requested records within 15 days (TMB Rule 163.3). The Legislature has continued to reinforce the entitlement in successive sessions: in 2025 it enacted House Bill 4224, which requires health care providers to post, plainly and publicly, how a patient may request their records and file a complaint when access is refused—a measure its Senate sponsors framed as ensuring that patients are "not only legally entitled to their health information but also practically able to obtain it" (2025). Access to one's health information is, in short, a right the state has recognized in statute, enforced through its licensing boards, and revisited as recently as the last legislative session.

Yet the interest at stake extends further than the electronic health record and the narrow question of whether a patient can retrieve and move it. The clinical file of diagnoses, laboratory results, and physician notes is only the most visible portion of a person's health information. A far larger and less legible body of health-related data is now generated outside the clinical encounter altogether: the readings logged by wearable devices and fitness trackers, the entries in wellness and fertility applications, the results returned by direct-to-consumer genetic tests, the symptom queries typed into search engines, the purchase and pharmacy histories that reveal a condition, and the location trails that record a visit to a provider. This information is health data in substance, whatever its statutory classification, and its downstream movement—its aggregation, inference, sale, and re-disclosure across a chain of recipients the patient will never encounter—lies almost entirely beyond the individual's control. Access and portability only describe the narrowest slice of the matter; the broader and more consequential question is one of control over the entirety of a person's own health-related information, wherever it originates and wherever it travels next.

At the center of the protected tier sits the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the nation's primary health-privacy law. HIPAA and its implementing regulations, the Privacy and Security Rules, establish national standards for the confidentiality of "protected health informa-

tion"—individually identifiable information, including the right to inspect and obtain copies of it (45 CFR Section 164.524). Crucially, however, HIPAA does not regulate health information as such. It regulates a defined and limited set of actors. Its protections attach only to "covered entities" (i.e., health plans, healthcare clearinghouses, and healthcare providers that transmit health information electronically in connection with certain transactions) and to the "business associates" that perform services for them (45 CFR Section 160.103). Everyone else falls outside the statute. As the Department of Health and Human Services itself acknowledged in a report to Congress (2016), health information effectively lives in two worlds: one regulated by HIPAA, and another, growing far faster, that is subject to no consistent privacy regulation at all.

The standard electronic health record begins its life in the first world. When a physician records a diagnosis or a laboratory returns a result, that information is created and held by a covered entity, and HIPAA's full apparatus of use limitations, disclosure restrictions, and patients' rights applies to it. The commercial health data described in the preceding section, by contrast, is generated in the second world and never enters the first. A heart rate captured by a smartwatch, a cycle logged in a fertility app, a genetic profile assembled by a testing company, or a health condition inferred from purchase history is health information every bit as sensitive as a chart note; however, because the entity that collects it is neither a covered entity nor a business associate, HIPAA never applies to it in the first instance (Theodos & Sittig, 2020). The same clinical datum can also cross from the first world into the second: once a patient, exercising the very access described above, downloads their record into a consumer application, or once a covered entity discloses information to a party outside the HIPAA chain, the data sheds its federal protection and enters the unregulated tier. Protection, in other words, is a function of who holds the data, not of what the data is or how sensitive it may be.

Long-known access and portability barriers now have collided with a second, faster-moving trend. As previous research has indicated, data collection, sale, and distribution practices have become more commonplace, lucrative, and precise (Dunmoyer & Whiting, 2022). While patients struggle to obtain their own information, a parallel commercial market has grown adept at collecting, processing, and trading it. The two have hybridized into an opaque digital-health economy in which one's health data is, in effect, alienated from the very person it describes—flowing to advertisers, analytics firms, and data brokers the patient will never see. The degree of public confusion that the alienation of this information produces is striking: two-thirds of U.S. adults (67%) say they understand little to nothing about what companies do with their personal data, up from 59% in 2019 (McClain et al., 2023). Most also feel powerless to do anything about it. A vast majority of Americans (73%) report having little to no control over what companies do with the data they collect (McClain et al., 2023).

The result is a system that fails patients twice over: it withholds their data from them while surrendering it to others. Federal regulators have repeatedly found consumer health platforms routing patients' most sensitive information to third parties. The Federal Trade Commission determined that the prescription-discount service GoodRx had shared users' prescription medications and personal health conditions with Facebook, Google, and other advertising companies, contrary to its own privacy promises (FTC, 2023). It separately barred the data broker X-Mode/Outlogic from selling precise location data that could reveal consumers' visits to medical and reproductive health clinics (FTC, 2024). Moreover, when the genetic-testing company 23andMe filed for Chapter 11 bankruptcy in March 2025, the genetic data of more than 15 million people who had been customers of the company became a salable asset (Ram et al., 2025).

This structural boundary—the point at which health information passes from HIPAA's protected tier into the unregulated commercial sphere—is the *HIPAA handoff*. This term is not entirely original to this paper, as the concept of a "HIPAA gap" has become established among health-privacy lawyers, regulators, and commentators, who use it to describe the widening body of consumer health data that falls outside HIPAA's institution-bound scope (see, e.g., Shachar, in Medscape, 2025; Jackson Lewis, 2025). Naming the gap is useful precisely because it locates the failure with specificity. The problem is not that health data is unregulated everywhere, but that a definitional line drawn in 1996 around a set of institutions no longer tracks where health information is practicably created, held, and moved.

LEGISLATION IN TEXAS

Texas has not been idle on data protections. Over the past two decades, the state has enacted a patchwork of statutes touching health and personal information, each addressing a piece of the problem and each, for present purposes, falling short of reaching health data across the HIPAA gap. Surveyed together, they reveal a framework that has built extensively on the protected side of the boundary while leaving the unprotected side largely untouched.

The Texas Medical Records Privacy Act (2011)

The Act, codified at Chapter 181 of the Health and Safety Code, is Texas's own analog to HIPAA, enacted on the view that the first proposed federal Privacy Rule did not go far enough. Its single most important feature is that it defines "covered entity" far more broadly than HIPAA, reaching any person who, for commercial, financial, or professional gain, assembles, collects, analyzes, uses, evaluates, stores, or transmits protected health information (Health and Safety Code Section 181.001). In principle, this is the breadth of scope the commercial data economy calls for. In practice, the Act's operative protections have been read and enforced chiefly against traditional healthcare actors, and its promise—a definition expansive enough to reach apps, vendors, and brokers—remains largely unrealized as an instrument against the downstream data trade. It is this dominant definition that the recommendations below propose to activate.

Consumer access guarantees (Chapter 181, Subchapter C; H.B. 4224, 2025)

Within the same chapter, Texas guarantees consumer access to electronic health records within 15 business days (Health and Safety Code Section 181.102) and, through House Bill 4224 in 2025, now requires covered entities to post clear instructions for requesting records and filing complaints (Health and Safety Code Section 181.105). These provisions strengthen the access right inside the clinical system but have no effect on data once it has left that system, and they impose no portability standard, format requirement, or fee cap.

The Texas Data Privacy and Security Act (2023)

The TDPSA, enacted as House Bill 4 and codified at Chapter 541 of the Business and Commerce Code, took effect on July 1, 2024, with its universal opt-out provision following on January 1, 2025 (HB 4, 2023). Popularly styled the "Texas Digital Bill of Rights," it made Texas one of the largest states to adopt a comprehensive consumer-privacy law and reflects a distinctly limited-government approach: rather than dictating how firms must operate, it vests enforceable rights in the individual and requires affirmative consent before the most sensitive categories of data may be used. The Act's core is a set of consumer rights: first, the right to know what data a business collects; second, the right to correct inaccurate information; third, the right to delete personal information; and fourth, the right to obtain data in a portable form (Business and Commerce Code, Section 541.051, 2023). To this, the statute adds the right to opt out of the processing of personal data as it regards targeted advertising, the sale of one's data, and certain automated profiling, as well as the right not to be penalized for exercising any of these (Section 541.051). The Act classifies health, genetic, and biometric information among its categories of "sensitive data," of which a business may not process without the consumer's opt-in consent (Section

541.001; Section 541.101). It defines the "sale" of personal data broadly, to exchanges for monetary or other valuable consideration (Section 541.001); forbids businesses from creating contracts or agreements that in any way waive or limit a consumer's rights as outlined in the Act (Section 541.054); and sets no revenue or volume threshold for coverage, exempting only small businesses as defined by the United States Small Business Administration (Section 541.107). Enforcement rests exclusively with the Attorney General, who may seek civil penalties of up to $7,500 per violation (Section 541.151; Section 541.155). For all its strength as consumer legislation, however, the TDPSA expressly exempts HIPAA-covered entities and protected health information—the exemptions examined in the next section—so that its considerable framework stops precisely at the health data boundary.

Supporting statutes

Three further laws address adjacent pieces of the problem. The Capture or Use of Biometric Identifiers Act governs the collection of biometric identifiers such as retina, fingerprint, and voiceprint data (Business and Commerce Code Chapter 503), but reaches only biometrics, not health data generally. The Texas Data Broker Act requires data brokers to register with the state and maintain safeguards (Business and Commerce Code Chapter 510), but its registration-and-security posture stops well short of restricting the sale of health-related data or requiring consumer consent for it. The Identity Theft Enforcement and Protection Act addresses data-security practices and breach notification (Business and Commerce Code Chapter 521), but speaks to safeguarding data against unauthorized acquisition, not to controlling authorized commercial trade of it.

Artificial-intelligence governance (2025)

Most recently, the Texas Responsible Artificial Intelligence Governance Act amended the TDPSA to clarify data-security duties for artificial-intelligence systems and other processors (HB 149, 2025). It refines obligations within the existing consumer-privacy framework but leaves the health data exemption intact.

Recent and unfinished efforts (89th Legislature, 2025)

The Legislature's continued attention to health data is itself evidence that the gap is recognized. The 89th Legislature considered Senate Bill 315 (2025), which would have formally recognized the heightened sensitivity of genetic information but did not pass. It did, however, enact Senate Bill 1188 (2025), which requires that electronic health records be physically stored within the United States and restricts access to such records strictly to personnel who need the information for treatment, payment, or healthcare operations. Nonetheless, SB 1188 answers only a jurisdictional concern and asserts limited role-based permissions, leaving questions on portability standards, downstream consent, and commercial data trade unanswered.

Against this state framework sits the federal floor on which Texas, like every state, continues to rely for clinical records: HIPAA, the information-blocking provisions of the 21st Century Cures Act, and the interoperability mandates of the Centers for Medicare and Medicaid Services. The pattern across the comprehensive survey is consistent. Texas has legislated capably and repeatedly on the protected side of the HIPAA handoff and around its periphery, but no existing Texas law extends access, portability, and downstream-control protections to health data once it crosses into the commercial sphere.

OPPORTUNITIES FOR IMPROVEMENT

For all its strengths, the TDPSA was not crafted to protect health data as it travels through the modern system, and upon inspection its limitations cluster around a single structural choice. The Act deliberately cedes the health sector to federal law. It exempts, at the entity level, any HIPAA-covered entity or business associate (Business and Commerce Code Section 541.002), and at the data level, it exempts protected health information, health records, and a long list of related categories (Section 541.003). The assump-

tion made was that HIPAA already governs health information—and within the clinical system, it does (45 CFR, Section 160.103). However, that assumption is precisely where the protection fails, because HIPAA applies only to the narrow list of institutions it deems covered entities and their business associates (Rockwern et al., 2021). The result is a system in which the clinical core is governed by HIPAA and the general consumer sphere is governed by the TDPSA, with a widening territory between them—the electronic-health-record vendors, patient portals, wellness and symptom applications, direct-to-consumer genetic services, and data brokers that receive health information after it exits a covered entity—that neither regime reaches. This gap is the HIPAA handoff: the moment data crosses out of the covered institution, federal protection ends and the TDPSA treats it, at most, as ordinary "sensitive data" subject to that Act's own limits (Section 541.003).

Those limits compound the problem. The portability right detailed in Section 541.051, while legitimate, is constrained to data the consumer "previously provided" and applies only where transfer is "technically feasible," carries no standardized format, fee cap, or response timeline, and—because health records are exempted—does little to help a patient actually move clinical information between providers (Cicero Institute, 2024). The Act's protection for sensitive health data, moreover, is keyed to a health "diagnosis"—language that a data broker assembling health inferences from purchases, search activity, or location can plausibly argue does not reach it, allowing opaque actors to slip the opt-in requirement altogether (Moore, 2025). The Act's safeguards for children stop at age 13, treating the data of adolescents aged 13 to 17 as that of ordinary adult consumers, while saying nothing about how patient portals should provision parental access or reconcile it with the narrow confidentiality the Family Code already affords minors (Cicero Institute, 2024). Its de-identified data exemption sits uneasily beside the well-documented ease of re-identifying genetic and location data (El Emam et al., 2011).

How data escapes: contracting around consumer rights in practice

The TDPSA forbids businesses from contracting around a consumer's rights (Business and Commerce Code Section 541.051), but that prohibition binds only entities the Act explicitly covers, while the mechanisms by which health data escapes protection operate largely among those it does not. In practice, "contracting around" a consumer's rights is not a single act but a set of routine industry practices. An application secures sweeping permissions through a terms-of-service agreement and privacy policy the user accepts with a single tap, burying authorization to "share data with partners" or "third parties" in language few read and even fewer understand. A data broker or analytics firm then acquires that data through a business-to-business contract to which the consumer is not a party and of which they have no notice, so that transfer is "authorized" without ever being meaningfully consented to. Aggregators combine data from many such sources and assert that the resulting product is "de-identified" and therefore unregulated, even where re-identification is feasible (El Emam et al., 2011). And when consent is nominally obtained, it is frequently extracted through interface designs—pre-checked boxes, confusing toggles, and consent flows engineered to steer the user toward disclosure (so-called dark patterns)—that secure a technical "yes" while defeating genuine choice (Ju et al., 2025). Each of these practices is lawful, or at least unaddressed, precisely because the actors performing them sit outside HIPAA and within the TDPSA's health exemption.

How the hidden movement of data harms the individual

Because these transfers are practically invisible to the patient, it is tempting to treat them as harmless. They are not. Health data that has left its protected institution can be used to set or deny insurance and set premiums; to inform employment and tenancy decisions through background and consumer-profiling products; and to target individuals at their most vulnerable, as when advertisers reach users inferred to be pregnant, depressed, or managing addiction.

Aggregated location and purchase data can expose deeply private facts—a visit to an oncologist, a psychiatric facility, or a substance-abuse program—to anyone willing to buy it. Unlike a compromised password, this information cannot be reset: a diagnosis or a genetic profile is permanent, and a genetic profile implicates blood relatives who never consented to its collection at all.

POLICY RECOMMENDATIONS

The shortfalls identified above are not arguments against the Texas Data Privacy and Security Act, nor in favor of imposing a sweeping federal-style regulatory regime. They are arguments for a set of targeted, incremental reforms that extend the Act's own principles—consent, transparency, and individual control—into the health-data context where they are most needed. Each recommendation below builds on instruments Texas already possesses or has drafted for adoption, and each is designed to restore patient ownership and control while preserving the competitive, innovation-friendly market that ultimately serves patients. Together, they pursue a single objective: ensuring that protection attaches to a Texan's health information itself, rather than to the institution that first holds it.

1. Strengthen patient portability of health records

Application. Texas should enhance patients' right to obtain and move their complete health records, secured through several mutually reinforcing measures. First, the State should make the intentional violation of the federal information-blocking rules actionable under Texas law (45 CFR Part 171, 2020)—treating the deliberate obstruction of a patient's access to their own records as an unlawful restraint of trade—and should render void any contractual term that restricts a patient or their representative from accessing those records. Second, Texas should extend the interoperability requirements of the federal Centers for Medicare and Medicaid Services (i.e., the patient-access, provider-directory, payer-to-payer, provider-access, and prior-authorization application interfaces) to the state-regulated insurers that the federal rules do not reach, so that the same access standards already binding on Medicare and Medicaid plans apply across the Texas market (CMS-0057-F, 2024). Third, the State should supply the concrete terms that make a portability right real rather than nominal: a response deadline of no more than 15 business days, a prohibition on fees for transmitting records electronically to the patient, or a patient-designated provider, an express provision that a system's "technical limitation" is no defense to noncompliance, and a requirement that records be furnished in a standardized, computable format.

What the format standards require. Two federal standards provide concrete guidelines for that format requirement. The United States Core Data for Interoperability (USCDI) is a standardized set of health data classes and constituent data elements—such as medications, laboratory results, clinical notes, and patient demographics—that a certified system must be able to exchange; it defines *what* information a portable record must contain so that a receiving system can recognize and use each element (Office of the National Coordinator for Health Information Technology, n.d.-a). Health Level Seven Fast Healthcare Interoperability Resources (HL7 FHIR) is the companion technical standard governing *how* that information is packaged and transmitted—an application programming interface specification that structures each data element into a consistent, machine-readable format retrievable by authorized applications (eCQI Resource Center, n.d.). Requiring both means a patient's record must not merely be handed over but delivered in a form another provider's system, or an application the patient chooses, can ingest and use, converting portability from a paper-copy right into wholly digital interoperability.

What it addresses. This recommendation directly remedies the thinness of the TDPSA's portability right, which is confined to data the consumer previously provided, excused where transfer is not "technically feasible," and inapplicable to exempt health records (Business and Commerce Code Section 541.003; Section 541.051). Furthermore, because information-

blocking is an anti-competitive practice, ensuring efficient and verifiable portability through enhanced interoperability measures promotes a free-market orientation: it treats vendor lock-in as the market failure it is, thereby restoring competition and patient choice rather than merely adding a compliance obligation.

2. Require affirmative patient consent before the resale or secondary use of health data

Application. Texas should prohibit any third-party recipient or data broker from selling, licensing, or using for a secondary purpose any identifiable health information without the patient's affirmative, specific, and revocable consent, and should bar the re-identification of health data that has been de-identified. Consent under this standard must be legitimate: obtained through a clear affirmative act separate from general terms of service, specific as to the categories of information, the purpose, and the categories of recipients, revocable through a method as accessible as the one by which it was given, and never secured through a dark pattern. The obligation travels with the data—each downstream recipient that transfers identifiable health information must bind the next by written agreement to the same limitations—so that a permission granted for one purpose cannot silently become authorization for another.

What it addresses. This is the foundational remedy for the HIPAA handoff. It reaches precisely the apps, vendors, and brokers that neither HIPAA nor the TDPSA's diagnosis-keyed sensitive-data rule effectively governs, and it directly answers the contracting practices identified above as the dark-pattern consent flow. Authoritative clinical guidance supports conditioning secondary use on meaningful, patient-respecting consent (Spector-Bagdady et al., 2023). By binding each recipient to the terms under which the data was first disclosed, the rule closes what is best understood as an issue with authorization transfer. The defect is not necessarily that the health data is shared, but that a permission given to one party, for one purpose, is presently allowed to expand—without the individual's knowledge or renewed consent—into uses and recipients that person never authorized.

3. Mandate auditability and role-based access

Application. For the portability and consent rights above to be meaningful, patients must be able to see who has interacted with their records. Texas should require electronic health record systems and patient portals serving Texans to implement role-based access controls that limit access to the minimum necessary for each user's role, to maintain tamper-evident audit logs of every access to and disclosure of a patient's records, and to furnish the patient, on request, a plain-language report of that access history.

What "provenance data" is. Texas does not need to devise this provenance tracking from scratch, because the federal USCDI standard already defines a *Provenance* data class. Provenance data is metadata (i.e., data about the data) that records the origin and chain of custody of each element in a health record: specifically, its *author* (the person or system that created the entry), the *author organization* responsible for it, and the *author time stamp* marking when it was created (Office of the National Coordinator for Health Information Technology, n.d.-b). In plain terms, provenance answers the questions *who created this piece of my record, on whose behalf, and when*—and, maintained over time, *who has since touched it*. It is the technical foundation of an audit trail. The same metadata that establishes a record's authenticity and integrity for clinical purposes can, when retained and surfaced to the patient, establish accountability for who has accessed and moved the record. (Office of the National Coordinator for Health Information Technology, n.d.).

What it addresses. Requiring certified systems serving Texans to populate and surface these existing provenance elements would give patients and auditors a standardized, interoperable account of who created or contributed to each entry and when, while imposing little additional collection burden, since that information already resides in the source system.

This answers the documented absence of consistent state standards for auditability and role permissions, makes that consent framework of Recommendation 2 verifiable rather than merely declared, and provides a practical check against unauthorized re-identification and misuse by making access visible and attributable (Zhang et al., 2011).

4. Secure parental rights over children's health records

Application. Texas should standardize parental and guardian access to a minor's health records, establishing default proxy access through patient portals, while automatically segmenting and withholding only those records arising from care to which a minor may lawfully consent independently under Chapter 32 of the Family Code, together with mental-health records protected under Chapter 611 of the Health and Safety Code.

What it addresses. This converts the abstract consent rules of existing law into an enforceable and uniform portal standard. It remedies the TDPSA's inability to protect adolescents between thirteen and seventeen, and the inconsistent, vendor-determined access decisions that families now encounter—decisions currently made not by law but by the default settings of whatever portal a practice happens to use (Chung et al., 2024).

5. Close the HIPAA gap by adopting the Texas definition of "covered entity"

Application. Finally, Texas should ensure that the duties above reach the actors federal law misses by anchoring them to the broader definition of "covered entity" already found in the Texas Medical Records Privacy Act (Health and Safety Code, 2011, Section 181.001), which extends to essentially any person who assembles, collects, analyzes, uses, stores, or transmits protected health information for commercial, financial, or professional gain, as opposed to simply the providers, plans, and clearinghouses to which HIPAA is confined.

What it addresses. Adopting this existing Texas definition as the operative scope for health data protection is the structural solution that gives the preceding four recommendations their reach across electronic health record vendors, portals, applications, and brokers; without it, each of the other protections would stop at the same institutional boundary that produces the gap in the first place. Because the definition is already enacted Texas law, the reform extends coverage without inventing a new regulatory category or agency—closing the gap with an instrument the state wrote for itself almost two decades ago.

Taken together, these recommendations extend the proven, consent-based logic of the Texas Digital Bill of Rights into health data, close the structural gap that has allowed protection to lapse at the clinical boundary, and make safeguards follow the information itself. They restore to Texans a genuine measure of ownership and control over their most personal data while preserving the open, competitive environment in which medical innovation continues to serve patients.

CONCLUSION

The inadequacy of health data protection this paper has described is not a failure of any single statute; rather, it is the lack of legal protection at the nexus of sensitive health information and consumer data practices. Existing federal and state safeguards attach to institutions (i.e., providers, health plans, and clearinghouses), whereas the information itself increasingly circulates beyond those institutions, among the applications, vendors, and data brokers that constitute the contemporary digital-health economy.

The consequence is one that the state has already half resolved. Texas has affirmed, repeatedly and recently, that patients hold a right to their health records, and has enforced that right inside the clinical system through access deadlines, licensing rules, and, as lately as 2025, new transparency mandates. However, it leaves those same patients without

protection the moment their data crosses the institutional line. A right recognized on one side of a boundary and abandoned on the other is a right only in part.

Texas is well positioned to resolve the issue of the HIPAA handoff, because it need not build the solution from scratch. The Legislature already possesses a comprehensive consumer-privacy statute premised on individual ownership of data, a statutory definition of "covered entity" broad enough to reach the commercial actors HIPAA misses, and a federal interoperability framework on which to model improved portability. What the foregoing analysis recommends is aligning these existing instruments toward a single end: that protection adhere to a patient's health information itself, and follow it—through transfers, secondary uses, and even bankruptcies—to whoever holds it next. The Legislature has already asserted that Texans own their data and are entitled to their records. Extending that declaration across the HIPAA gap, so that ownership and control mean as much as the clinic within it, is the unfinished work this paper advises it to complete. Protection should follow the data, not the institution.■

REFERENCES

45 C.F.R. § 160.103. https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-160/subpart-A/section-160.103

45 C.F.R. pt. 171. https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-D/part-171

Capture or Use of Biometric Identifiers Act, Tex. Bus. & Com. Code § 503.001 (2007). https://statutes.capitol.texas.gov/Docs/BC/htm/BC.503.htm

Chung, R. J., Lee, J. B., Hackell, J. M., & Alderman, E. M. (2024). Confidentiality in the care of adolescents: Technical report. *Pediatrics, 153*(5), e2024066327. https://doi.org/10.1542/peds.2024-066327

Cicero Institute. (2024). *Model electronic health record legislation.* https://ciceroinstitute.org/wp-content/uploads/2024/10/2025-Model-EHR-Bill-Fall-2025-Annotated.pdf

Dunmoyer, D., & Whiting, B. (2022, September 15). *Why Texas needs a digital bill of rights.* Texas Public Policy Foundation. https://www.texaspolicy.com/why-texas-needs-a-digital-bill-of-rights/

eCQI Resource Center. (n.d.). *FHIR—Fast Healthcare Interoperability Resources: About.* Retrieved July 30, 2026, from https://ecqi.healthit.gov/fhir/about

El Emam, K., Jonker, E., Arbuckle, L., & Malin, B. (2011). A systematic review of re-identification attacks on health data. *PLOS ONE, 6*(12), e28071. https://doi.org/10.1371/journal.pone.0028071

Federal Trade Commission. (2023, February 1). *FTC enforcement action to bar GoodRx from sharing consumers' sensitive health info for advertising* [Press release]. https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-enforcement-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising

Federal Trade Commission. (2024, January 9). *FTC order prohibits data broker X-Mode Social and Outlogic from selling sensitive location data* [Press release]. https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-prohibits-data-broker-x-mode-social-outlogic-selling-sensitive-location-data

HB 4. Enrolled. 88th Texas Legislature. Regular. (2023). https://capitol.texas.gov/tlodocs/88R/billtext/html/HB00004F.htm

HB 149. Enrolled. 89th Texas Legislature. Regular. (2025). https://capitol.texas.gov/tlodocs/89R/billtext/html/HB00149F.htm

Ju, I., Ham, C. D., & Yel, E. (2026). Dark Patterns in Data-Consent Disclosures and Consumer Reactance to Online Behavioral Advertising. *Journal of Advertising*, *55*(3), 307–325. https://doi.org/10.1080/00913367.2025.2593666

Identity Theft Enforcement and Protection Act, Tex. Bus. & Com. Code § 521.001 et seq. (2007). https://statutes.capitol.texas.gov/Docs/BC/htm/BC.521.htm

Lazzarotti, J. J. & Silver, D. W. (2025, May 27). *States move forward with privacy protections to close HIPAA gaps for health, reproductive health info*. Jackson Lewis. https://www.jacksonlewis.com/insights/states-move-forward-privacy-protections-close-hipaa-gaps-health-reproductive-health-info

McClain, C., Faverio, M., Anderson, M., & Park, E. (2023, October 18). *How Americans view data privacy.* Pew Research Center. https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/

Medicare and Medicaid Programs; Patient Protection and Affordable Care Act; Advancing Interoperability and Improving Prior Authorization Processes, 89 Fed. Reg. 8758 (Feb. 8, 2024). https://www.federalregister.gov/documents/2024/02/08/2024-00895/medicare-and-medicaid-programs-patient-protection-and-affordable-care-act-advancing-interoperability

Moore, H. (2025). De-identified and unregulated: How data brokers outpace state privacy laws. *Vanderbilt Journal of Entertainment and Technology Law, 27*(4), 863. https://scholarship.law.vanderbilt.edu/jetlaw/vol27/iss4/6/

Office of the National Coordinator for Health Information Technology. (n.d.-a). *United States Core Data for Interoperability (USCDI)*. Retrieved July 30, 2026, from https://isp.healthit.gov/united-states-core-data-interoperability-uscdi

Office of the National Coordinator for Health Information Technology. (n.d.-b). *United States Core Data for Interoperability (USCDI).* Retrieved July 30, 2026, from https://isp.healthit.gov/uscdi-data-class/provenance

Ram, N., Prince, A. E. R., Roberts, J. L., Fox, D., & Spector-Bagdady, K. (2025). The precarious future of consumer genetic privacy. *Science, 389*(6765), 1092–1094. https://doi.org/10.1126/science.adz7229

Rockwern, B., Johnson, D., & Snyder Sulmasy, L. (2021). Health information privacy, protection, and use in the expanding digital health ecosystem: A position paper of the American College of Physicians. *Annals of Internal Medicine, 174*(7), 994–998. https://pubmed.ncbi.nlm.nih.gov/33900797/

SB 315. Introduced. 89th Texas Legislature. Regular. (2025). https://capitol.texas.gov/tlodocs/89R/billtext/pdf/SB00315I.pdf

SB 1188. Enrolled. 89th Texas Legislature. Regular. (2025). https://capitol.texas.gov/tlodocs/89R/billtext/pdf/SB01188F.pdf

Spector-Bagdady, K., et al. (2023). Principles for health information collection, sharing, and use: A policy statement from the American Heart Association. *Circulation, 148*(13), 1061–1069. https://doi.org/10.1161/CIR.0000000000001173

Tex. Fam. Code § 32.001 et seq. https://statutes.capitol.texas.gov/Docs/FA/htm/FA.32.htm

Tex. Health & Safety Code § 611.001 et seq. https://statutes.capitol.texas.gov/Docs/HS/htm/HS.611.htm

Texas Data Broker Act, Tex. Bus. & Com. Code § 510.001 et seq. (2023). https://statutes.capitol.texas.gov/?tab=1&code=BC&chapter=BC.510&artSec=

Texas Data Privacy and Security Act, Tex. Bus. & Com. Code § 541.001 et seq. (2023). https://statutes.capitol.texas.gov/Docs/BC/htm/BC.541.htm

Texas Medical Records Privacy Act, Tex. Health & Safety Code § 181.001 et seq. (2001). https://statutes.capitol.texas.gov/Docs/HS/htm/HS.181.htm

Theodos, K., & Sittig, S. (2020). Health Information Privacy Laws in the Digital Age: HIPAA Doesn't Apply. *Perspectives in health information management*, *18*(Winter), 1l. https://pmc.ncbi.nlm.nih.gov/articles/PMC7883355/

Trivedi, N., et al. (2021). Barriers to accessing online medical records in the United States. *The American Journal of Managed Care*, *27*(1), 33 – 40. https://doi.org/10.37765/ajmc.2021.88575

U.S. Department of Health and Human Services. (2016). *2016 report to congress on health IT progress: examining the hitech era and the future of health IT* [Report]. https://healthit.gov/wp-content/uploads/2025/08/2016_report_to_congress_on_healthit_progress.pdf

Weber, S. (2025, November 18). *More states adopt consumer privacy laws to address HIPAA gaps*. Medscape. https://www.medscape.com/viewarticle/more-states-adopt-consumer-privacy-laws-address-hipaa-gaps-2025a1000w3h?form=fpf

Zhang W, Gunter CA, Liebovitz D, Tian J, Malin B. (2011). Role prediction using Electronic Medical Record system audits. *AMIA … Annual Symposium proceedings. AMIA Symposium, 2011,* 858– 867. https://pmc.ncbi.nlm.nih.gov/articles/PMC3243238/

ABOUT THE AUTHORS

Brooke Garner is a Healthcare Policy Scholar at the Texas Public Policy Foundation, where she advances patient-centered healthcare reforms shaped by her own experience navigating barriers within the healthcare system. After personally facing delays and obstacles to timely care, Brooke became committed to restoring a model that prioritizes patient choice, affordability, and transparency in Texas.

She previously served as a Healthcare Policy Analyst Intern at the Foundation, where she published two op-eds and was honored as Intern of the Year. She later served as a Campus Ambassador, supporting student engagement with the Foundation's mission.

Brooke graduated from the University of Arkansas with a B.A. in Political Science and minors in Spanish and Legal Studies. While at Arkansas, she was a member of Zeta Tau Alpha, the Political Science Honors Society, and the National Society of Leadership and Success. She was also selected for both the Winthrop Rockefeller Civic Leadership Academy and the Health Reformers Academy Fellowship, where she further developed her focus on healthcare reform and civic leadership.

Charlie Glover is an intern with the Healthy Texas Initiative at the Texas Public Policy Foundation, where her research focuses on patient access to electronic health records, health-data privacy, and interoperability in Texas law. She is a political science student at Texas A&M University's Bush School of Government and Public Service, with minors in philosophy and legal foundations.

Texas Public
POLICY FOUNDATION

901 Congress Avenue | Austin, Texas 78701 | (512) 472-2700 | www.TexasPolicy.com