Journal of Legal Medicine

The Jurisprudence of Clinical Information

Legal Ownership, Access, and Control of Healthcare Data in the United States

Healthcare Facility Legal Counsel Reference Guide for Software & Data

The digital transformation of the American healthcare system has fundamentally challenged the traditional paradigms of data ownership and information control. In the contemporary legal landscape, the concept of "owning" healthcare data—specifically Protected Health Information (PHI) and Electronic Health Information (EHI)—is less about property rights in the classical sense and more about a complex bundle of rights and obligations distributed among patients, healthcare providers, and technology developers. While physical or electronic medical records have historically been viewed as the property of the physician or hospital that created them, a series of federal and state legislative maneuvers, most notably the Health Insurance Portability and Accountability Act (HIPAA) and the 21st Century Cures Act, have recalibrated this balance, effectively granting patients a sovereign right of control over the information that documents their biological existence.[1, 2]

Software Developer: Roadmap for Data Rights & Control

Navigating the landscape of US healthcare data law requires a transition from viewing data as a static record to viewing it as a dynamic, rights-bearing asset. The patient's right of access is the apex right, which Covered Entities and software developers must facilitate through APIs and interoperable standards.[1, 11] Ownership remains a functional reality for the provider but is legally subordinate to the patient's sovereign right of control.[2]

Implications for Software Architecture

To remain compliant in 2025 and beyond, healthcare software must implement:

1. **Granular Export Capabilities:** Systems must be able to export the entire DRS, not just the USCDI v1 data elements, in machine-readable formats to avoid information blocking.[9, 12]
2. **State-Aware Logic:** Platforms operating in multiple states must adjust access response times (5 days in CA, 15 in TX, 30 in others) and storage locations based on the patient's residency.[8, 30, 37]
3. **AI Transparency Layers:** AI must include user-facing disclosures and documented physician-review logs to satisfy SB 1188 and AB 3030.[34, 42, 45]
4. **Privacy-by-Design Consent:** Consent management must be modular to handle Washington MHMDA's separate opt-ins for collection, sharing, and selling.[50, 54]

As data monetization for AI training expands, de-identification via Expert Determination remains the most viable pathway for secondary use without individual authorization.[16, 17, 19] However, the rise of "Shadow AI" and "Prompt Leaking" as recognized data breach categories in 2026 suggests that the security perimeter must now extend to the AI interface itself.[24] Software developers who prioritize these data rights and security safeguards will not only mitigate legal risk but will also gain a competitive advantage in a market increasingly defined by patient trust and data interoperability.

The Federal Baseline: HIPAA and the Legal Fiction of Ownership

The foundational regulatory framework for health data privacy in the United States is the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Despite its ubiquity, HIPAA does not explicitly establish who "owns" healthcare data. Instead, it focuses on the protection of PHI and the rights of individuals to access it.[2, 3] In the absence of a federal ownership statute, the legal consensus has evolved into a bifurcated model: healthcare providers own the physical or digital media containing the records, while patients possess the legal, enforceable right to the information contained within those records.[2, 4]

The Right of Access under 45 CFR § 164.524

The HIPAA Privacy Rule, specifically 45 CFR § 164.524, serves as the primary mechanism for patient control. It establishes that individuals have a right to inspect and obtain copies of their PHI maintained in a "Designated Record Set" (DRS) for as long as the information is maintained by a Covered Entity or their Business Associate.[3, 5, 6] This right is fundamental to patient autonomy, enabling individuals to take responsibility for their care, identify medical identity theft, and contribute their data to research.[4, 6]

Component of HIPAA Right of Access	Description and Scope
Designated Record Set (DRS)	Medical records, billing records, enrollment, payment, claims adjudication, and any record used to make decisions about individuals.[3, 6]
Response Timeline	Covered entities must act on a request within 30 days, with a single 30- day extension permitted if a written delay notice is provided.[3, 5, 7]
Format Requirements	Must be provided in the form and format requested if "readily producible"; electronic PHI must be provided in electronic format if requested.[3, 5, 6]

Cost-Based Fees	Entities may charge only reasonable, cost-based fees for labor (copying/postage) and supplies; searching and retrieval fees are prohibited.[3, 7, 8]
Verification	Actors must take reasonable steps to verify identity without creating "unreasonable barriers" to access.[3, 6]

The scope of the DRS is expansive, including not only clinical notes and lab results but also x-rays, wellness program files, and clinical case notes.[3] However, the right of access excludes psychotherapy notes and information compiled in anticipation of litigation.[3, 6, 7] For a software developer, understanding the boundaries of the DRS is critical, as any system designed to hold patient-facing data must be capable of exporting the full breadth of the DRS to satisfy a request.[3, 9]

Limitations of Ownership by Covered Entities

From a provider's perspective, the "ownership" of a medical record reflects the investment of resources into compiling, managing, and storing the data.[2] Clinicians are entitled to maintain original records for treatment continuity, legal defense, and administrative compliance. However, this ownership is conditional and secondary to the patient's right of access.[2, 4] Covered entities cannot withhold records due to unpaid bills, nor can they impose unreasonable procedural barriers, such as requiring a patient to physically visit an office when electronic transmission is feasible.[3, 9]

The 21st Century Cures Act: From Access to Interoperability

If HIPAA established the right to a copy of data, the 21st Century Cures Act of 2016 established the right to the *flow* of data. This legislation identifies that health data is a fluid asset that must be accessible across the healthcare continuum to improve outcomes and reduce costs.[1, 10] The Cures Act explicitly targets "information blocking"—practices that interfere with the access, exchange, or use of Electronic Health Information (EHI).[1, 11, 12]

The Information Blocking Mandate

The Information Blocking Rule (45 CFR Part 171) applies to three "actors": healthcare providers, health IT developers of certified health IT, and health information exchanges/networks.[1, 12] The law creates a shift in the power dynamic by making the sharing of EHI the "expected norm".[11, 12] Practices such as charging excessive fees for data exports, requiring unnecessary contracts, or causing extended delays are now considered unlawful information blocking.[9, 13]

For software developers, the Cures Act mandates the adoption of standardized Application Programming Interfaces (APIs). This ensures that patients can securely access their structured EHI using smartphone applications of their choice.[11, 14] The definition of EHI has been expanded beyond the HIPAA "ePHI" to include all electronic information that would be in a DRS, further reducing the ability of hospitals to

gatekeep data.[12]

Reasonable and Necessary Exceptions

The ONC has codified specific exceptions where withholding or restricting EHI does not constitute information blocking. These exceptions provide a safe harbor for actors to protect patient safety or system integrity.[12, 13]

Exception Category	Purpose	Examples of Qualifying Actions
Preventing Harm	To protect patients from unreasonable risk of physical harm.	Delaying the release of a result until a physician can discuss a life-altering diagnosis with the patient.[12]
Privacy	To comply with state or federal privacy laws requiring consent.	Not sharing data when a patient has explicitly requested a restriction or when a state law requires a signed opt-in.[12]
Security	To safeguard the confidentiality and integrity of EHI.	Implementing a temporary block to investigate a suspected cybersecurity breach.[12]
Infeasibility	To account for technical or uncontrollable limitations.	Inability to fulfill a request due to a natural disaster or lack of tech capability to segment data.[12]
Health IT Performance	To maintain system functionality.	Taking a portal offline for scheduled maintenance or performance upgrades.[12]
Manner Exception	Provide flexibility in data delivery.i	If the requested API is not technically supported. provide data via a secure file transfer [12]

These exceptions are narrow and require documentation. For instance, the "Infeasibility Exception" requires a written response to the requestor within ten business days explaining why the request cannot be met.[12] Software platforms must therefore include administrative modules to track and document these justifications.[15]

Data for AI and Commercial Use: Monetization and Compliance

The intersection of healthcare data and artificial intelligence represents a significant commercial opportunity for software companies. However, the legal requirements for utilizing patient data for AI model training or commercial product development are stringent, requiring a nuanced understanding of de-identification and patient authorization.[16, 17, 18]

De-identification as a Regulatory Threshold

According to 45 CFR § 164.514, once health information is properly de-identified, it is no longer considered PHI and is exempt from HIPAA's restrictions.[16, 19] This is the primary path for large-scale AI development. HIPAA recognizes two methods of de-identification:

1. **Safe Harbor Method:** This requires the removal of 18 specific identifiers, including names, precise geographic data, and all dates more specific than a year.[16, 19, 20] While simple to implement, it often renders data less useful for AI models that rely on temporal patterns or localized trends.[16, 17]
2. **Expert Determination Method:** A qualified expert uses statistical and scientific principles to certify that the risk of re-identification is "very small".[16, 17, 19] This method allows for the retention of more data (like granular dates or locations) if the risk is mathematically mitigated, providing higher fidelity for machine learning.[17, 20]

Authorization for the "Sale of PHI"

If the data is not de-identified, any exchange of PHI for direct or indirect remuneration is considered a "Sale of PHI" and requires specific patient authorization.[18, 21] This authorization must explicitly state that the disclosure will result in remuneration to the Covered Entity.[18, 21, 22] Notably, hospitals cannot condition treatment on a patient signing an authorization for the sale of their data.[18, 22]

Modern Business Associate Agreements (BAAs) in 2025/2026

As of 2025, the standard Business Associate Agreement is being overhauled to address the risks of AI. Modern BAAs for AI vendors now frequently include:

- **No-Retention Clauses:** Prohibiting the vendor from using PHI to train or fine-tune its foundational models once the specific service is complete.[23, 24]
- **Audit Rights for AI Logs:** Allowing Covered Entities to audit not just the data storage, but the AI prompts and outputs to ensure no PHI "leaked" into the model's memory.[24, 25]
- **Re-identification Warranties:** Legally binding the vendor not to attempt to link de-identified data sets back to individuals using external data sources.[23, 24]
- **Enhanced Encryption Standards:** Requiring TLS 1.2+ for all API calls and encryption of ePHI both at rest and in transit.[20, 23, 24]

State-Level Variations: The Fragmentation of Data Sovereignty

While federal law provides a baseline, a "patchwork" of state laws imposes stricter requirements. When state law provides greater privacy protection or more expansive patient rights, it preempts HIPAA.[8, 26, 27, 28]

Texas: TMRPA, HB 300, and SB 1188

Texas has enacted some of the nation's most robust medical privacy laws. The Texas Medical Records Privacy Act (TMRPA) expanded the definition of a Covered Entity to include virtually anyone who handles

PHI, regardless of their role in the healthcare system.[8, 26, 29]

Texas Legislative Provision	Requirement for Software Developers / Providers
HB 300 (Access Speed)	Must provide electronic records within 15 business days of a request.[8, 26, 29]
SB 1188 (US Storage)	Effective Jan 1, 2026, all EHRs containing Texas resident data must be physically stored in the US or its territories.[30, 31, 32]
SB 1188 (AI Disclosure)	Practitioners using AI for diagnostics must disclose such use to patients.[33, 34, 35]
SB 1188 (EHR Data Fields)	Prohibits storing credit scores or voter registration in EHRs; requires a biological sex field.[30, 36]
Training Mandate	Employees must be trained on state/federal laws by the 90th day of hire.[26, 29]

Texas law also imposes significant civil penalties, reaching up to $250,000 per violation for intentional disclosures for financial gain.[8, 26, 29] The domestic storage requirement (SB 1188) is a critical consideration for software firms using offshore cloud servers.[30, 32]

California: CMIA and the CCPA/CPRA

California's framework, led by the Confidentiality of Medical Information Act (CMIA), is unique for its private right of action, allowing patients to sue for negligent disclosures even without proving specific intent.[27, 37, 38]

- **Accelerated Access:** Under the Patient Access to Health Records Act (PAHRA), California providers must respond to access requests within 5 days.[27, 37]
- **CCPA/CPRA Integration:** While HIPAA data is largely exempt, the CCPA applies to non-PHI data such as tracking pixels on health websites or data from wellness apps.[27, 37, 39] Consumers have rights to delete, correct, and opt-out of the "sharing" of their data.[39, 40]
- **SB 1120 (Physicians Make Decisions Act):** Effective Jan 1, 2025, health insurers cannot use AI algorithms alone to deny care. A licensed physician must review any adverse determination.[41, 42, 43, 44]
- **AB 3030 (GenAI Disclaimers):** Any clinic or physician's office using generative AI to communicate clinical information must include a disclaimer indicating AI was used.[42, 45, 46]

Washington: The My Health My Data Act (MHMDA)

Washington's MHMDA is currently the nation's strictest health privacy law, targeting the "gap" in data collected by entities not covered by HIPAA (e.g., health apps, wearables, and retailers).[47, 48, 49]

- **Broad "Health Data" Definition:** Includes any data that can identify a consumer's physical or mental health status, including location data revealing an attempt to seek healthcare.[47, 50, 51, 52]
- **Opt-In Consent:** Entities must obtain affirmative opt-in consent before collecting or sharing consumer health data.[48, 51, 53, 54]
- **Geofencing Prohibition:** It is unlawful to implement a geofence around healthcare facilities to track or send messages to consumers seeking care.[47, 51, 52]
- **Enforcement:** MHMDA provides a private right of action with statutory damages and attorney fees, creating a high litigation risk for non-compliant software firms.[55, 56, 57]

AI Bias, Safety, and the Regulatory Response

As AI becomes central to clinical decision support, regulators are moving to ensure these tools do not exacerbate health disparities. Both federal and state authorities are introducing standards for bias testing and human oversight.[20, 58, 59]

Bias Mitigation and Impact Assessments

California's AB 331 (and its reintroductions as AB 2930) aims to regulate Automated Decision Tools (ADTs). These bills require "impact assessments" to determine if an algorithm shows a preference based on race, sex, or age.[60, 61, 62] Software developers are increasingly required to provide "technical documentation" and "visualization dashboards" to prove their algorithms are explainable and fair.[63]

Similarly, Colorado's AI Act requires "deployers" (like health insurers) to notify individuals of AI-generated consequential decisions and provide a right to appeal.[64] In these jurisdictions, software must be architected to include "human-in-the-loop" overrides for any AI-driven diagnostic or treatment recommendation.[20, 65, 66]

Data Security and Breach Notification Standards

The definition of a "breach" and the timeline for notification are tightening across the United States. While HIPAA allows 60 days, states are moving toward 15-day and 30-day windows.[67, 68, 69]

Jurisdiction	Breach Notification Deadline	Specific Requirements
HIPAA (Federal)	**60 Days.[70, 71]**	Notice to individuals, HHS, and media if >500 residents.[70, 71]

New York (SHIELD)	**30 Days.[69, 72]**	Firm 30-day cap; includes medical/health insurance info as "private info".[69, 73]
California	**15 - 30 Days.[67, 68]**	Sample notice to AG within 15 days if >500 residents.[68]
Texas	**60 Days.[8, 26]**	Notify Texas AG if >250 residents.[8, 26]
Pennsylvania	**72 Hours.[67]**	One of the fastest notification windows in the US.[67]

For a software development company, the "date of discovery" is the critical trigger. Modern security rules require multifactor authentication (MFA), network segmentation, and penetration testing every 12 months to prevent unauthorized access to ePHI. [20, 24, 41]

PQC+™

Transformativ IP

Regulatory Compliance & HNDL Protection
Federal & all 50 States within 90 Days

www.TransformativIP.ai
Info@TransformativIP.ai

73 Endnotes and References

1. Guide to the 21st Century Cures Act for Healthcare IT Compliance - Access, https://www.accesscorp.com/blog/guide-to-the-21st-century-cures-act/

2. The need for clear medical data ownership laws - PMC, https://pmc.ncbi.nlm.nih.gov/articles/PMC12763853/

3. Individuals' Right under HIPAA to Access their Health Information 45 ..., https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html

4. Patient Rights Under HIPAA - Updated for 2026, https://www.hipaajournal.com/hipaa-rights/

5. 45 CFR § 164.524 - Access of individuals to protected health information., https://www.law.cornell.edu/cfr/text/45/164.524

6. Individuals' Right under HIPAA to Access their Health Information | HHS... Page 1 of 22 - Orange Coast College, http://www.orangecoastcollege.edu/about_occ/Accreditation/2019_Institutional_Self_Evaluation_Report/Ev idence/Standard_II_C/II.C.8-10_Student_Health_Center_HIPAA.pdf

7. HIPAA and the Right of Access: A Q&A for Covered Entities - Coates' Canons - UNC, https:// canons.sog.unc.edu/2023/02/hipaa-and-the-right-of-access-a-qa-for-covered-entities/

8. Physician's Guide to Privacy & Medical Records Laws in Texas, https://www.99mgmt.com/blog/medical-records-laws-in-texas

9. Accessing Electronic Health Information Cures Act - Munson Healthcare, https://www.munsonhealthcare.org/new-patient-portals/accessing-electronic-health-information-cures-act **10.** Health Information Blocking: Responses Under the 21st Century Cures Act - PMC, https://pmc.ncbi.nlm.nih.gov/articles/PMC6134556/

11. ONC's Cures Act Final Rule - ASTP - Assistant Secretary for Technology Policy, https://healthit.gov/regulations/cures-act-final-rule/

12. Information Blocking - ASTP - Assistant Secretary for Technology.https://healthit.gov/information-blocking/

13. 21st Century Cures Act -- Information Blocking & Rule Summary - Harmony Healthcare IT, https://www.harmonyhit.com/21st-century-cures-act-information-blocking-rule-summary/

14. 21st Century Cures Act Compliance for HIPAA Covered Entities, https://www.hipaajournal.com/cures-act-compliance/

15. The 21st Century Cures Act and Information Blocking - MagMutual, https://www.magmutual.com/healthcare-insights/article/21st-century-cures-act-and-information-blocking

16. Can de-identified data be used to train AI under HIPAA? - Paubox, https://www.paubox.com/blog/can-de-identified-data-be-used-to-train-ai-under-hipaa

17. Synthesizing healthcare data for AI model training, with HIPAA Expert Determination, https://www.tonic.ai/guides/hipaa-ai-compliance

18. HIPAA: Individual Authorization Is Required Before Any Sale of PHI - Accountable, https://www.accountablehq.com/post/hipaa-individual-authorization-is-required-before-any-sale-of-phi

19. Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule | HHS.gov,

https://www.hhs.gov/hipaa/ for-professionals/special-topics/de-identification/index.html

20. HIPAA Compliance AI in 2025: Critical Security Requirements You Can't Ignore - SPRY, https://www.sprypt.com/blog/hipaa-compliance-ai-in-2025-critical-security-requirements

21. HIPAA Marketing and Sale Provisions: Legal Potholes for Providers, Payors, Advertisers, Data Aggregators, Market Researchers and Others - Duane Morris,

https://www.duanemorris.com/alerts/HIPAA_Marketing_and_Sale_Provisions_4851.html

22. Guide to HIPAA for Covered Entities - Americares,

https://www.americares.org/wp-content/uploads/globalassets/_snc/eduresources/practicefacility/hipaa/3. - hipaa-guide-may-2014.pdf

23. Business Associate Agreements in 2025: Are Patient Data Protections Keeping Up with AI?, https:// mdrxlaw.com/news-and-alerts/business-associate-agreements-in-2025-are-patient-data-protections-keeping/

24. AI Risk Management for HIPAA Privacy Rule Compliance | Censinet, Inc.,

https://censinet.com/perspectives/ai-risk-management-hipaa-privacy-rule-compliance

25. HIPAA 2026: AI Agents for OCR Audit Contract Evidence - Sirion,

https://www.sirion.ai/library/contract-insights/hipaa-ai-agents-contract-evidence-ocr-audits/

26. What is Texas HB300? Updated for 2026 - The HIPAA Journal,

https://www.hipaajournal.com/what-is-texas-hb-300/

27. Mandatory Medical Privacy Regulations in California You Must Comply With, https://www.hipaajournal.com/medical-privacy-regulations-california/

28. What HIPAA Laws Protect vs State Privacy Laws (CMIA, HB300, CPRA): 2025 Guide, https://www.accountablehq.com/post/what-hipaa-laws-protect-vs-state-privacy-laws-cmia-hb300-cpra-2025-guide

29. Texas HB 300 (Texas Medical Privacy Act) Explained: Requirements, Training, and Penalties - Accountable,

https://www.accountablehq.com/post/texas-hb-300-texas-medical-privacy-act-explained-requirements-train ing-and-penalties

30. From PHI to AI What Texas SB 1188 Means for Healthcare Entities and Vendors | Buchalter, https:// www.buchalter.com/insights/from-phi-to-ai-what-texas-sb-1188-means-for-healthcare-entities-and-vendors/

31. SB 1188 - 89th Legislature - Texas Policy Research,

https://www.texaspolicyresearch.com/bills/89th-legislature-sb-1188/

32. Texas Enacts Electronic Health Record Data Localization Law - Hunton Andrews Kurth LLP, https://www.hunton.com/privacy-and-cybersecurity-law-blog/texas-enacts-electronic-health-record-data-loc alization law

33. Mandatory Medical Privacy Regulations in Texas You Must Enforce Across Your Organization - The HIPAA Journal, https://www.hipaajournal.com/medical-privacy-regulations-in-texas/

34. New Law Requires Texas Physicians to Disclose AI, Provide Guardians EHR Access, https://www.texmed.org/Template.aspx?id=66759

35. New Texas AI Healthcare Laws: SB 1188 & HB 149 Compliance Guide,

https://www.hchlawyers.com/blog/2026/february/new-texas-laws-require-ai-disclosure-in-healthca/

36. 89(R) SB 1188 - Committee Report (Unamended) version - Bill Analysis,

https://capitol.texas.gov/tlodocs/89R/analysis/html/SB01188H.htm

37. Complying with HIPAA California Law - Updated for 2026,

https://www.hipaajournal.com/hipaa-california-law/

38. California Confidentiality of Medical Information Act vs. HIPAA - ZenGRC,

https://www.zengrc.com/blog/california-confidentiality-of-medical-information-act-vs-hipaa/

39. CCPA penalties and fines: What are the consequences of noncompliance? - Usercentrics, https://usercentrics.com/knowledge-hub/ccpa-penalties/

40. CCPA Penalties: What Happens If You Don't Comply? - Pandectes GDPR Compliance, https://pandectes.io/blog/ccpa-penalties-what-happens-if-you-dont-comply/

41. The 2024 Year in Review: Cybersecurity, AI, and Privacy Developments - Hinckley Allen, https://www.hinckleyallen.com/publications/the-2024-year-in-review-cybersecurity-ai-and-privacy-developments/

42. Healthcare AI 2025 - USA -- California | Global Practice Guides - Chambers and Partners, https://practiceguides.chambers.com/practice-guides/healthcare-ai-2025/usa-california/trends-and-developments

43. California Limits AI Use by Health Plans - Vita Companies, https://vitacompanies.com/blog/california-limits-ai-use-by-health-plans

44. Bill Text: CA SB1120 | 2023-2024 | Regular Session | Chaptered - LegiScan, https://legiscan.com/CA/text/SB1120/id/3023335

45. GenAI Notification Requirements | Medical Board of California, https://www.mbc.ca.gov/Resources/Medical-Resources/GenAI-Notification.aspx

46. The Big Long List of U.S. AI Laws | News - Taft Law, https://www.taftlaw.com/news-events/news/the-big-long-list-of-u-s-ai-laws/

47. Washington's My Health My Data Act | Emery Reddy, https://www.emeryreddy.com/data-breach/washingtons-my-health-my-data-act

48. HIPAA vs MHMDA - Privado AI, https://www.privado.ai/post/hipaa-vs-mhmda

49. Washington State Privacy Law: My Health, My Data Act - Compliancy Group, https://compliancy-group.com/washington-state-privacy-law/

50. Washington State Passes My Health My Data Act | Blog - OneTrust, https://www.onetrust.com/blog/washington-state-passes-my-health-my-data-act/

51. Time to Comply: Washington My Health My Data Act | BCLP, https://www.bclplaw.com/en-US/events-insights-news/time-to-comply-washington-my-health-my-data-act.html

52. Washington State Imposes Far-Reaching Privacy Obligations for Consumer Health Data, https://www.hklaw.com/en/insights/publications/2023/05/washington-state-imposes-far-reaching-privacy-o bligations

53. How state laws are beefing up health data privacy protections - Healthcare Brew, https://www.healthcare-brew.com/stories/2025/10/28/tate-laws-beefing-up-health-data-privacy-protections

54. How State Laws Shape Digital Health Privacy | Censinet, Inc., https://censinet.com/perspectives/state-laws-shape-digital-health-privacy

55. Data protection laws in the United States, https://www.dlapiperdataprotection.com/?c=US

56. My Health My Data Act (MHMD) - Perkins Coie, https://perkinscoie.com/services/my-health-my-data-act-mhmd

57. My Health, My Data, My Class Action Lawsuit: Why the Washington My Health My Data Act Deserves EVERY Company's Attention | Wyrick Robbins Practical Privacy, https://practicalprivacy.wyrick.com/blog/my-health-my-data-my-class-action-lawsuit-why-the-washington-m y health-my-data-act-deserves-every-companys-attention

58. Artificial Intelligence Regulations: State and Federal AI Laws 2026 - Drata, https://drata.com/blog/artificial-intelligence-regulations-state-and-federal-ai-laws-2026

59. Governing AI in Mental Health: 50-State Legislative Review - PMC, https://pmc.ncbi.nlm.nih.gov/articles/PMC12578431/

60. California's Proposed Artificial Intelligence Anti-Discrimination Bill - SHRM, https://www.shrm.org/topics tools/tools/express-requests/california-s-proposed-artificial-intelligence-anti-d iscriminatio

61. Time for California to Act on Algorithmic Discrimination | TechPolicy.Press, https:// www.techpolicy.press/time-for-california-to-act-on-algorithmic-discrimination/

62. Assemblymember Bauer Kahan's AB 331 Regulating Automated Decision Tools Passes Committee | Official Website, https://a16.asmdc.org/press-releases/20230411-assemblymember-bauer-kahans-ab-331-regulating-autom a ted-decision-tools

63. CA Legislator to Revive AI Anti Discrimination Bill in 2025 - Baker McKenzie, https:// www.bakermckenzie.com/-/media/files/people/newman-bradford/ca-legislator-to-revive-ai-anti-disc rimination-bill-in-2025.pdf?ref=compliancehub.wiki

64. State AI Health Tracker | Holland & Knight, https://www.hklaw.com/en/general-pages/state-ai-health-tracker

65. Trump's Executive Order on AI and the Potential Impact on State Healthcare Laws Governing AI - Maynard Nexsen, https://www.maynardnexsen.com/publication-trumps-executive-order-on-ai-and-the-potential-impact-on-s t ate-healthcare-laws-governing-ai

66. AHA Response to HHS RFI on AI in Health Care, https://www.aha.org/lettercomment/2026-02-23-aha-response-hhs-rfi-ai-health-care

67. Laws Protecting Your Health Data: Complete Guide (2026) | HealthConsent, https://myhealthconsent.org/privacy-guide/legal-framework

68. 2025 Breach Notification Law Update - Perkins Coie, https://perkinscoie.com/insights/update/2025-breach-notification-law-update

69. A MoFo Privacy Minute: New York Data Breach Notification | Morrison Foerster, https:// www.mofo.com/resources/insights/250314-a-mofo-privacy-minute-new-york-data-breach-notification

70. HIPAA Breach Notification Rule | American Medical Association, https://www.ama-assn.org/practice-management/hipaa/hipaa-breach-notification-rule

71. Breach Notification Rule | HHS.gov, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

72. New Year, New Data Breach Notification Requirements in New York: Impactful Changes for Life Sciences and Consumer Health Care Companies | Insights | Ropes & Gray LLP, https://www.ropesgray.com/en/insights/alerts/2025/01/new-year-new-data-breach-notification-requiremen ts in-new-york

73. New York Amends its Data Breach Notification Law | Byte Back, https://www.bytebacklaw.com/2025/02/new-york-amends-its-data-breach-notification-law/