OMNITEK CONSULTING

Privacy Infrastructure Across Jurisdictions

WHITE PAPER

Building One Compliance Engine for a Patchwork of State Health Data Laws

Abstract

Twenty states now have comprehensive privacy laws in effect, three of them, Indiana, Kentucky, and Rhode Island, joining the landscape in 2026 alone, each with its own definitions, consent requirements, and enforcement mechanisms. For life sciences organizations, the sharpest edge of that patchwork is Washington's My Health My Data Act, which broadens what counts as regulated health data well beyond HIPAA's scope, requires explicit consumer authorization before that data is sold or shared, and backs its enforcement with both the state Attorney General and a private right of action for individual litigants. California's Privacy Protection Agency has made the financial stakes concrete, reaching a $2.75 million settlement with Disney entities in February 2026, its largest CCPA settlement to date, following a $1.4 million settlement with a mobile gaming company months earlier. A pharmaceutical or medical device company collecting patient, caregiver, or healthcare provider data across even a handful of states is now navigating requirements that can differ meaningfully from one state line to the next. This white paper applies established data governance best practices, already proven in reconciling the state transparency reporting patchwork, to a practical approach for privacy compliance across the same fragmented landscape.

A Patchwork That Looks Familiar, Applied to a Different Kind of Data

Life sciences compliance teams have already lived through one version of this problem. State transparency reporting laws layered on top of the federal Sunshine Act created a patchwork where the same payment had to be reported differently depending on which state a recipient practiced in. Privacy law is following an almost identical pattern, except the data at stake is not payment information. It is patient data, caregiver data, and healthcare provider data, collected through websites, patient support programs, market research, and commercial field activity, now subject to a rapidly expanding set of state requirements that were mostly written without pharmaceutical or medical device use cases specifically in mind.

Twenty states now have comprehensive privacy laws on the books, and the pace of new legislation is not slowing. Three states, Indiana, Kentucky, and Rhode Island, added new comprehensive privacy laws effective in 2026 alone, while several existing state frameworks underwent amendments ahead of their own effective dates the same year.[i] An organization that built its privacy compliance program around a handful of early-adopter states is very likely already behind the current landscape, whether or not anyone inside the organization has noticed yet.

Why Health Data Specifically Raises the Stakes

Washington's My Health My Data Act deserves specific attention from any life sciences organization, because it defines health data far more broadly than HIPAA does and applies regardless of whether the organization is a HIPAA-covered entity. The law requires explicit consumer authorization before health data is sold or shared, imposes transparency requirements around how that data is used, and backs enforcement with both the state Attorney General and a private right of action available to individual consumers.[ii] That last detail matters enormously for risk calculus. A private right of action means the organization's compliance exposure is not limited to regulatory enforcement priorities. It extends to any individual consumer with standing to sue, a meaningfully different risk profile than a law enforced solely by a state agency with finite investigative capacity.

Pharmaceutical companies running patient support programs, disease awareness campaigns, or digital engagement tools that touch health-adjacent data, even data that never enters a formal medical record, are squarely inside the kind of activity Washington's law was written to capture. An organization that has mapped its compliance obligations only against HIPAA is very likely missing exposure that a broader, consumer-protection-style health data law like Washington's creates.

The Enforcement Signal Getting Harder to Ignore

California's Privacy Protection Agency has moved decisively from theoretical enforcement authority to real financial consequences. Its February 2026 settlement with Disney entities, at $2.75 million, stands as the largest CCPA settlement reached to date, following a $1.4 million settlement with a mobile gaming company in late 2025 and a further settlement with a sports streaming platform in March 2026.[iii] The pattern across these actions establishes something compliance and legal teams should treat as settled precedent rather than a remote risk: multi-million-dollar penalties for privacy violations are no longer theoretical, and the agencies enforcing them are demonstrably willing to pursue them.

None of the settlements reached so far specifically targeted a life sciences organization, but the enforcement pattern does not suggest the industry is exempt. A pharmaceutical or medical device company handling the kind of sensitive consumer and health data that triggered these actions in other industries carries comparable, and in some respects heightened, exposure, particularly given how directly health data sits at the center of laws like Washington's.

Applying Best Practices: One Privacy Compliance Engine, Not Fifty

Established data governance best practice solves exactly this shape of problem for state transparency reporting: one data model, one jurisdictional map, and one configurable rules layer that absorbs new requirements instead of triggering a rebuild every time a new state acts. Applied to privacy compliance, the same architecture extends into four specific capabilities.

1. **A Single Data Inventory Mapped Against Every Applicable Jurisdiction.** Build one comprehensive inventory of what personal and health data the organization collects, and map it against the specific requirements of every state where that data originates, rather than maintaining separate, disconnected compliance efforts per state.
2. **A Configurable Consent and Rights Layer.** Build consent capture, disclosure, and consumer rights fulfillment as a configurable rules engine that can absorb a new state's specific requirements without requiring a new system, mirroring exactly the approach already applied to transparency reporting.
3. **Health Data Flagged as Its Own Risk Tier.** Given how much more broadly laws like Washington's define health data compared to HIPAA, and the private right of action risk that comes with it, treat health-adjacent data as a distinct, higher-scrutiny category within the broader privacy data model rather than folding it into general consumer data governance.
4. **A Standing Legislative Monitoring Function.** With new comprehensive state privacy laws arriving on an ongoing basis, build a standing process for tracking new and amended state requirements, so the compliance engine's rules layer gets updated proactively rather than discovered reactively.

None of this requires building a new system from scratch for every state that acts. It requires the same discipline already applied to transparency reporting: one underlying architecture, extended and reconfigured as the jurisdictional landscape evolves, rather than a new point solution for every new law.

What One Compliance Engine Buys, and Where It Gets Hard

Advantages

- **Faster response to new state laws:** a configurable rules layer absorbs a new state's specific requirements in weeks rather than requiring a new compliance project each time legislation passes.
- **Reduced exposure to private right of action risk:** explicit health data risk tiering ensures the highest-stakes data category gets the scrutiny its heightened litigation exposure warrants.
- **A defensible, documented compliance posture:** a single data inventory mapped against jurisdictional requirements gives legal and compliance teams a clear, current answer when asked what the organization actually does with a specific category of data.

- **Lower long-term compliance cost:** one reusable architecture is cheaper to maintain and extend over time than a series of disconnected, state-specific compliance efforts built independently.

Risks and Barriers

- **Data inventory complexity:** many life sciences organizations do not have a complete, current picture of every place personal and health data enters the organization, and building that inventory is a genuine undertaking before any compliance engine can be built on top of it.
- **Cross-functional ownership:** privacy compliance data flows through marketing, commercial, medical affairs, and IT systems that rarely report to a single leader, and building shared ownership takes deliberate governance work.
- **Legislative pace outrunning implementation:** with new state laws arriving continuously, a compliance engine needs genuine agility built in, not just a one-time build, to keep pace with a landscape that is not slowing down.
- **Conservative interpretation costs:** in ambiguous cases, particularly around what counts as health data under broader state definitions, a genuinely conservative compliance posture may limit some commercial or marketing activities the organization would otherwise want to pursue.

Case in Point: The Patient Support Program That Outgrew Its Compliance Map

A mid-size specialty pharmaceutical company ran a digital patient support program collecting enrollment, adherence, and engagement data across all fifty states, with a privacy compliance framework built primarily around HIPAA and California's privacy law, the two frameworks the company's legal team had prioritized when the program launched. When Washington's My Health My Data Act took effect, the company had not reassessed the program against it, reasoning that the program was not a HIPAA-covered activity and assuming HIPAA-adjacent compliance was sufficient.

A subsequent privacy audit found that several categories of data the program collected, including inferences about a patient's health status drawn from engagement patterns, fell within Washington's considerably broader definition of health data, and that the program's consent flow did not meet the law's explicit authorization requirement for that category. The company had to rebuild its consent architecture specifically for Washington residents and conduct a retrospective review of data already collected, a remediation effort that a jurisdictional mapping exercise, built proactively when the law was first enacted, would have avoided entirely.

Recommendations for Privacy and Compliance Leaders

1. **Build a complete data inventory before building anything else.** compliance mapping is only as good as the underlying picture of what data the organization actually collects and where.
2. **Map every jurisdiction where the organization has consumer or patient reach.** not just the handful of states with the most established privacy laws or the most media attention.
3. **Treat health-adjacent data as its own risk tier.** given how much more broadly laws like Washington's My Health My Data Act define health data compared to HIPAA.

4. **Build a standing legislative monitoring function.** rather than discovering a new state's requirements only after an audit or a complaint surfaces the gap.
5. **Assign clear cross-functional ownership of privacy compliance.** spanning marketing, commercial, medical affairs, and IT, since data flows through all of them.
6. **Review consent architecture against private-right-of-action states specifically.** given the materially different risk profile a state law with individual litigant standing creates compared to agency-only enforcement.

Measuring Success: KPIs for Privacy Infrastructure Maturity

- **Jurisdictional coverage completeness:** the percentage of states with applicable privacy requirements that have been explicitly mapped against the organization's data inventory.
- **Time to compliance for new state laws:** the average time between a new state privacy law taking effect and the organization's compliance engine reflecting its specific requirements.
- **Health data risk tier coverage:** the percentage of health-adjacent data flows explicitly reviewed against the broadest applicable state health data definitions.
- **Consent architecture audit pass rate:** the percentage of consumer-facing data collection points that pass a periodic audit against current state consent requirements.

Conclusion

Twenty states with comprehensive privacy laws, three new ones arriving in a single year, and a health-data-specific law in Washington that reaches well beyond HIPAA's boundaries describe a compliance landscape that has genuinely outgrown a patchwork response. California's willingness to pursue multi-million-dollar CCPA settlements confirms the enforcement risk is real, not theoretical, and the private right of action embedded in laws like Washington's means that risk extends beyond what any single regulator chooses to prioritize.

Carrying disciplined best practices from transparency reporting into privacy compliance means applying the same underlying discipline to a different data domain: one inventory, one jurisdictional map, one configurable rules layer built to absorb the next state law rather than require a new project for it. Organizations that build that infrastructure now are choosing to get ahead of a landscape that is still actively expanding, rather than discovering its gaps during an audit, an inspection, or a lawsuit.

About OmniTek & Contact Information

OmniTek Consulting is a trusted partner for organizations seeking to enhance governance, operational agility, and decision-making. We specialize in modernizing business processes with a blend of human-centered design, technology expertise, and hands-on change management.

For privacy and compliance leaders managing patient, caregiver, and provider data across a growing patchwork of state requirements, OmniTek applies proven best practices to build a practical privacy compliance engine: a complete data inventory, jurisdictional mapping, health data risk tiering, and standing legislative monitoring.

Whether you are building this infrastructure for the first time or responding to a gap a recent state law already exposed, OmniTek can help you build a compliance posture that scales with the patchwork instead of chasing it.

Contact us today to explore how OmniTek can support your transformation journey and drive lasting results.

McLean, VA | Serving clients nationwide
info@omnitekconsulting.com
omnitekconsulting.com

Click here to book a 15-minute call to see how OmniTek can help your team put these insights into practice.

Endnotes

[i] MultiState, "All of the Comprehensive Privacy Laws That Take Effect in 2026", available at https://www.multistate.us/insider/2026/2/4/all-of-the-comprehensive-privacy-laws-that-take-effect-in-2026

[ii] DTC Perspectives, "FOFO: Fear of Finding Out and the Impact of the Washington My Health My Data Act on Pharmaceutical Company Compliance", available at https://www.dtcperspectives.com/fofo-fear-of-finding-out-and-the-impact-of-the-washington-my-health-my-data-act-on-pharmaceutical-company-compliance/

[iii] ComplianceHub.Wiki, "Twenty States, One Patchwork: The 2026 State Privacy Map and Why Enforcement Just Got Real", available at https://compliancehub.wiki/2026-state-privacy-law-patchwork-20-states-cppa-enforcement-escalation/