News|**Articles**|July 10, 2026

New obstacles for healthcare: Federal and state national security regulations increasingly target health data

*Author(s)*Kate Black , Mason Fitch

Health systems, life sciences companies and laboratories face new rules, which carry penalties for violations. Here are strategies for dealing with new regulations on health data.

Over the past three years, federal and state regulations aimed at preventing foreign adversary access to American health and genomic data have grown into a multi-layered framework.

Kate Black and Mason Fitch

The DOJ's Bulk Sensitive Data Rule, state laws in Florida, Texas, and Utah, impose data localization mandates, remote access bans, and equipment restrictions — yet remain largely unaligned.

For life sciences companies, clinical laboratories, telehealth platforms, and consumer health brands, the question is no longer whether these obligations apply, but how many apply at once and where to allocate resources.

The regulatory landscape: Enacted laws

The DOJ Bulk Sensitive Data Rule (enforceable as of October 6, 2025). Restricts access to U.S. sensitive personal data—including health, genomic, and biometric data and biospecimens—by a "country of concern" (China, Russia, Iran, North Korea, Cuba, or Venezuela) or linked "covered person." In-scope companies must maintain a written compliance program with due diligence, risk-based reviews, auditing, and 10-year recordkeeping.

Florida Electronic Health Records Exchange Act (effective July 1, 2023). Requires Florida providers using certified EHR technology to ensure offsite patient data—including

data held by vendors or cloud providers—is physically stored in the continental U.S., its territories, or Canada.

Texas Genomic Act of 2025, (effective September 1, 2025). Prohibits companies, medical or research facilities, and nonprofits from using genome sequencers or sequencing-related software produced by or for a foreign adversary (including subsidiaries and affiliates). Genomic data of Texas residents must be stored in the U.S. and inaccessible from within adversary borders. Requires annual AG compliance certification and creates a private right of action.

Utah Genetic Information Amendments (effective January 1, 2028; penalties May 1, 2028). Bans genetic sequencers and operational or research software produced by or affiliated with foreign adversaries, prohibits storage of genetic data within adversary borders, and requires prohibited equipment to be removed or permanently disabled and replaced with compliant alternatives.

Comparing the Four Regimes

Scope and data types. The DOJ Rule is broadest, covering any U.S. person or entity in transactions involving health data (10,000+ records), genomic data (100+), biometric data (1,000+), and biospecimens. Texas and Utah focus on genome and genetic sequencing data at companies, medical and research facilities, and nonprofits. Florida's EHR Act covers all qualified EHR data but only for Florida-licensed providers using certified EHR technology.

Equipment and software restrictions. The DOJ Rule and Florida EHR Act impose no hardware or software bans. Texas prohibits genome sequencers and sequencing-related software produced by or for a foreign adversary, including subsidiaries and affiliates. Utah goes further, requiring prohibited equipment and software to be physically removed or permanently disabled and replaced.

Data storage and foreign adversary designations. The DOJ Rule treats any agreement giving a country of concern access to bulk U.S. sensitive personal data as a restricted "covered data transaction." Texas and Utah require U.S.-based storage inaccessible from within adversary borders. Florida permits storage in the continental U.S., its territories, or Canada. All four target the same six adversary nations — China, Russia, Iran, North Korea, Cuba, and Venezuela — except Florida, which uses a geographic mandate rather than naming countries.

Enforcement and penalties. Texas alone provides a private right of action (up to $5,000 per violation) and AG enforcement up to $10,000. The DOJ Rule carries the steepest penalties: civil fines up to $377,700 and criminal penalties up to $1 million and 20 years'

imprisonment. Utah allows $10,000 per violation plus actual damages, enforced solely by the AG. Florida relies on the Agency for Health Care Administration discipline.

Certification and compliance reporting. The DOJ Rule requires annual internal audits, with certification requirements varying by transaction type. Texas requires attorney-prepared annual certification to the AG by December 31. Utah requires a sworn statement by December 31, 2028, with recertification every 10 years. Florida requires attestation under penalty of perjury at licensure or renewal.

Practical compliance roadmap for life sciences, healthcare, and consumer health organizations

These laws may appear narrow but likely affect most health, life science, and biotech companies. A nationwide telehealth platform offering a consumer genetic test, or a life sciences company operating Texas and Florida labs, running clinical trials with genomic data, or marketing a consumer genetic product, may be subject to all four regimes at once. Organizations should:

Determine which laws apply. Map operations, data flows, and patient populations against each law's jurisdictional triggers, including any vendor or collaborator relationships with entities linked to foreign adversary countries.

Verify data storage and access controls. Conduct an independent review of where health and genomic data is physically stored and who has remote access, encompassing primary repositories, backup locations, cloud infrastructure, and any offshore support teams.

Analyze research and clinical trial exceptions. The DOJ Rule includes limited exemptions for clinical research and regulatory approvals; Texas provides a narrow exception for HIPAA-defined research. Determine whether any exceptions apply and document them.

Audit equipment and software supply chains. Inventory all genome sequencing hardware and software, tracing each item's manufacturer, country of production, and corporate parentage to identify foreign adversary links. Texas requires immediate cessation of use; Utah will require removal or replacement by January 1, 2028.

Update vendor contracts. Incorporate required federal and state provisions into vendor agreements. Require periodic recertification of vendor compliance, conduct risk-based audits of high-risk vendors, and maintain records sufficient to support Texas's annual AG certification and the DOJ Rule's 10-year recordkeeping requirement.

Address Texas-specific litigation risk. Companies processing genomic data of Texas residents should quantify exposure, evaluate insurance coverage for statutory damages, and ensure compliance is robust enough to defend against potential suits.

The outlook: Pending state legislation

State-level action is accelerating. In early 2026, several additional states introduced or advanced similar legislation, including West Virginia, Wisconsin, and Virginia. Companies that invest in compliance infrastructure now will be prepared not only for today's requirements, but for the additional state laws as well.

Kate Black is a partner at Kelley Drye. Mason Fitch is special counsel at Kellye Drye.

https://www.chiefhealthcareexecutive.com/view/new-obstacles-for-healthcare-federal-and-state-national-security-regulations-increasingly-target-health-data