Insights, News & Events

AI COMPANY'S ACQUISITION OF GENETIC TESTING FIRM SPARKS LANDMARK PRIVACY LAWSUIT – WHAT EMPLOYERS AND MEDTECH SHOULD KNOW

Insights
Apr 22, 2026

AI Company's Acquisition of Genetic Testing Firm Sparks Landmark Privacy Lawsuit – What Employers and MedTech Should Know

A recent Illinois federal class action lawsuit alleges an AI healthcare company obtained health data during a corporate acquisition and shared that data with biotech and pharmaceutical companies in violation of key privacy laws. MedTech companies and their business customers should pay attention. The April 15 lawsuit targets Tempus AI, a Chicago-based healthcare technology company, and stems from its February 2025 acquisition of a genetic testing firm with a database of more than one million genetic tests. The plaintiffs allege that Tempus AI compelled the acquired firm to hand over its entire cache of genetic testing data shortly after the acquisition and then licensed their data to more than 70 pharmaceutical and biotech partners through agreements totaling more than $1.1 billion, all without providing notice, much less obtaining the written consent of the patients. What do employers and MedTech companies need to know about this new avenue of attack we'll likely be seeing more of in the near future?

What the Lawsuit Alleges

Seven named plaintiffs from states across the country (Illinois, California, New York, Michigan, Florida, Georgia, and West Virginia) claim that they provided their genetic information to Ambry Genetics Corporation for medical testing purposes with the expectation that it would be kept

Related People

James C. Fessenden
Partner

858.597.9600

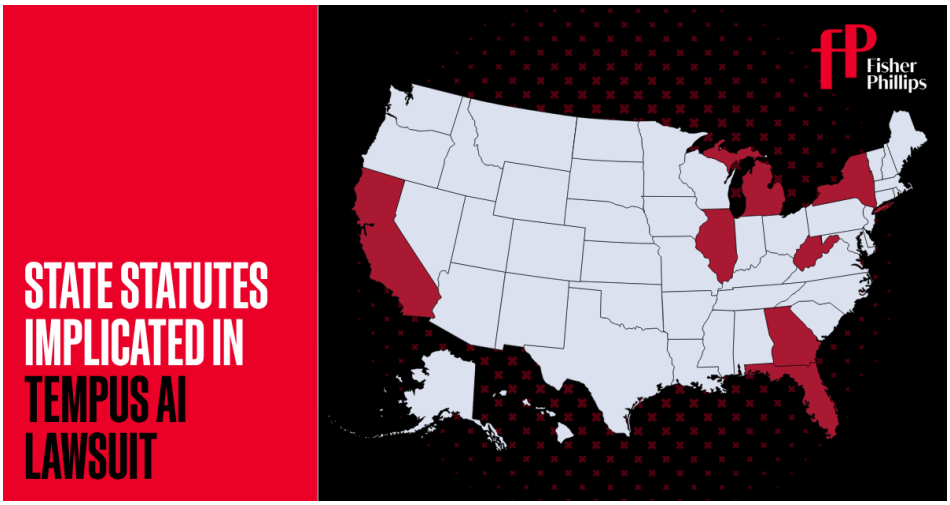
Danielle Kays
Partner

312.260.4751

confidential. When Tempus AI completed its $600 million acquisition of Ambry, the suit alleges, their data was swept up and transferred without notice or consent, then commercially exploited as training data for Tempus AI's artificial intelligence tools and as a licensed dataset for third-party life sciences companies.

> **Important caveat:** These are simply allegations in a civil complaint. Tempus AI has not yet had the opportunity to respond, and nothing in this lawsuit has been proven in court. The company may have defenses (legal, factual, or both) that have not yet been presented, so read this summary with a grain of salt.

The complaint alleges Tempus AI's revenue grew more than 83% year-over-year in 2025, and attributes much of that growth to the commercialization of the Ambry genetic data. The plaintiffs further allege that Tempus AI's public statements that it only shares "de-identified" data don't hold up. They argue genetic data is inherently identifiable and cannot be meaningfully anonymized, regardless of what labels are stripped away.



The legal claims span a wide range of state statutes: Illinois's Genetic Information Privacy Act (GIPA), the California Confidentiality of Medical Information Act, and consumer protection laws in Florida, Georgia, Michigan, New York, and West Virginia. The complaint also includes common law claims for negligence, unjust enrichment, fraudulent concealment, conversion, invasion of privacy, breach of contract, and breach of fiduciary duty.

The Genetic Data Angle

Service Focus

AI, Data, and Analytics

Litigation and Trials

Mergers and Acquisitions

Privacy and Cyber

Industry Focus

Healthcare

Life Sciences and Pharma

Tech

Resource Hubs

AI Governance Hub

Related Offices

Chicago

What makes this case particularly consequential is the nature of the data involved. Genetic information occupies a uniquely sensitive category under the law. Plaintiffs allege Congress recognized that when it passed the Genetic Information Nondiscrimination Act (GINA) in 2008. Unlike a Social Security number that can be changed or a password that can be reset, your DNA is permanent, deeply personal, and predictive of health conditions that extend to your biological relatives. More than a dozen states have enacted additional genetic privacy protections since then.

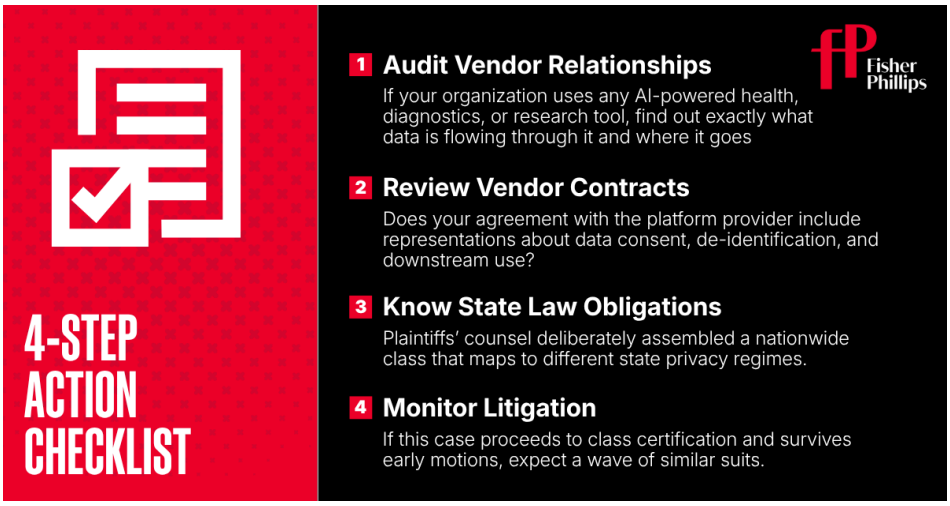
Illinois's GIPA, the lead statute in this case, is among the most stringent. It requires written authorization before genetic testing results can be disclosed to anyone other than the tested individual. The statute provides for statutory damages of $15,000 per intentional or reckless violation, or $2,500 per negligent violation. With a class potentially numbering in the hundreds of thousands, the exposure in a case like this may be staggering.

Why This Case Could Be an Inflection Point

If you've been following AI-related privacy litigation over the past two years, this case might look familiar. The pattern mirrors what we saw with AI call recording and transcription services: lawsuits against the platform developers came first, followed quickly by suits against their enterprise customers: the companies that purchased and deployed those tools.

The Tempus AI complaint is notable because the company serves major healthcare systems, research institutions, and life sciences companies, and it has publicly touted the breadth of its data-sharing partnerships. In prior litigation waves, plaintiffs' attorneys have used vendor websites, press releases, and earnings calls to identify downstream customers, arguing that those customers either knew or should have known that the platforms they were using had legal exposure.

Healthcare and MedTech companies that license AI-powered diagnostic, research, or clinical decision-support tools may be drawn into litigation as a named defendant simply by virtue of being a known customer.



4 Things Employers and MedTech Companies Should Do Now

- First, **audit your AI vendor relationships**. If your organization uses any AI-powered health, diagnostics, or research tool, find out exactly what data is flowing through it and where it goes, including whether that data is used to train models or licensed to third parties.
- Second, **review your vendor contracts**. Does your agreement with the platform provider include representations about data consent, de-identification, and downstream use? What data can vendors' employees access? Are there indemnification provisions that would protect your organization if the vendor's practices are later found to be unlawful?
- Third, **know your state law obligations**. Plaintiffs' counsel deliberately assembled a nationwide class that maps to different state privacy regimes. If you operate in California, Illinois, New York, or other states with robust genetic or health data privacy laws, you are at higher risk and have a greater obligation to stay up to speed on local requirements.
- Fourth, **monitor the litigation**. If this case proceeds to class certification and survives early motions, expect a wave of similar suits targeting not just platform developers but healthcare employers and MedTech companies that incorporated AI tools trained on patient data without verified consent. The best way to stay up to speed is to ensure you are subscribed to Fisher Phillips' Insight System.

Conclusion

We will continue to monitor developments related to this litigation, so make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information. If you have questions, contact your Fisher Phillips attorney, the authors of this Insight, or any member of our Privacy and Cyber Team, our Life Sciences and Pharma Team, or our Tech Sector Team.