

Federal and State Data Restrictions Are Forcing Health Systems to Re-Examine Where Clinical Documentation Is Produced

A federal national security rule, a growing set of state statutes, and mounting physician edit burden are converging.

NEW YORK, NY, UNITED STATES, September 16, 2026 /EINPresswire.com/ -- For two decades, the

“

The important thing for health systems to understand is that these are separate obligations with separate triggers.”

James Maisel, MD, Founder & CEO of ZyDoc

economics of U.S. medical transcription pointed offshore. A significant share of American clinical documentation has been produced outside the United States, and for most of that period no federal rule prohibited it. HIPAA sets standards for safeguarding protected health information, but it does not restrict where that information is stored or processed.

That has changed, and health systems are now reexamining long-standing arrangements.

What the Rules Now Require

Two separate bodies of law are driving the shift.

At the federal level, the Department of Justice's Data Security Program (28 C.F.R. Part 202), issued under Executive Order 14117, took effect April 8, 2025. The rule prohibits and restricts transactions that give countries of concern or covered persons access to bulk U.S. sensitive personal data, including personal health data. Analysts note that data de-identified under HIPAA may still fall within scope if it meets the rule's bulk thresholds. Due diligence, audit, and reporting obligations have phased in on their own schedule, and DOJ has advised organizations to know both their data and their vendors.

State requirements are more direct, and two states have written them into statute.

Florida Senate Bill 264, effective July 1, 2023, requires providers using certified electronic health record technology to keep all patient information physically within the continental United States, its territories, or Canada. It reaches third-party and subcontracted facilities and cloud providers, and licensees must attest to compliance at initial licensure and each renewal.

Texas Senate Bill 1188 followed. Most provisions took effect September 1, 2025. Its data localization requirement took effect January 1, 2026, requiring electronic health records under a covered entity's control to be physically maintained in the United States or a U.S. territory. It applies regardless of when the record was created, reaches third-party vendors and cloud providers, and carries civil penalties. Analysts note that Texas's broad definition of covered entity reaches well beyond traditional clinical settings.

Where State Restrictions Apply

Restrictions fall into three tiers, and many organizations face more than one.

Statutes restricting offshore storage of health records, applying broadly to providers:

Florida (SB 264)

Texas (SB 1188)

State Medicaid programs expressly prohibiting offshore storage or processing of Medicaid data, usually by executive order or contract:

Alaska

Arizona

Ohio

Wisconsin

States imposing restrictions, conditions, or attestation requirements on offshore subcontracting involving patient data:

Arizona

Florida

Georgia

Mississippi

Missouri

New Jersey

Ohio

Tennessee

Texas

Several other state Medicaid agencies permit offshore processing only under specific conditions. Alaska, Arizona, Missouri, New Jersey, Ohio, and Wisconsin also broadly prohibit offshore performance in state contracting, and individual solicitations sometimes bar offshore work where no statute requires it. Commercial payer contracts vary, and some require an offshore subcontracting attestation and annual audits of the offshore vendor.

Classifications differ by source and change often. An organization treating patients from a restricting state may face that state's scrutiny even if it operates elsewhere, so providers should verify current requirements everywhere they are licensed or treat patients.

"The important thing for health systems to understand is that these are separate obligations with separate triggers," said James M. Maisel, MD, Founder and CEO of [ZyDoc®](#). "A vendor can be fully HIPAA compliant and still create exposure under a state residency statute or a federal national security rule. Compliance is no longer a single question with a single answer, and the contracts most organizations signed years ago were not written with any of this in mind."

The Second Pressure: The Note Still Comes Back to the Physician

This comes just as providers reassess AI-only documentation tools.

Ambient and AI-only scribing tools make it easy to capture an encounter and draft a note. But the draft still returns to the clinician for review, correction, and sign-off, so much of the burden is deferred rather than removed. Industry estimates put physician time correcting AI-generated documentation at more than 80 minutes a day. Undercoding and insurance clawbacks tied to incomplete documentation exceed \$1 billion annually.

Many organizations now evaluate documentation vendors on two axes: where the work is performed, and how much of it lands back on the clinician.

"Health systems are being asked to solve a compliance problem and a workforce problem with the same contract," said Matt Koerner, Chief Marketing Officer and Strategic Advisor at ZyDoc®. "Those used to be separate conversations handled by separate people, and they are one conversation now."

He points to a further question underneath both.

"The one almost nobody has answered yet is who is responsible for data security at signoff," he said. "A note can pass through an AI system, a vendor, a subcontractor, and a cloud environment before it comes back to the physician for final approval. By the time the clinician signs,

accountability has been spread across so many hands that it is not clear who owns it. We need to address it quickly, as an industry, while we still have room to do it thoughtfully."

Questions Provider Organizations Should Be Asking

Documentation and compliance leaders may want to confirm the following with any vendor handling clinical documentation:

- Where is the work performed, including by subcontractors?
- Where is patient data stored, and where is it accessible?
- Does the business associate agreement address data residency, or only safeguards?
- Can the vendor support a state residency attestation?
- Has the vendor assessed its exposure under 28 C.F.R. Part 202?
- How much clinician time is required after the note is returned?
- Is the output EHR-ready?
- At signoff, who is responsible for the record's security?

Organizations should consult qualified healthcare counsel about their specific circumstances, as requirements vary by state, licensure type, and data involved.

About ZyDoc®

ZyDoc® is a U.S.-based clinical documentation company serving physician practices, ambulatory surgery centers, and healthcare organizations nationwide. It combines advanced AI with expert U.S.-based human oversight to deliver accurate, secure, workflow-friendly documentation without offshore risk. Learn more at <https://www.zydoc.com>.

This release is provided for general informational purposes and does not constitute legal advice.

Matthew Koerner, MM, MBA

ZyDoc

+1 800-546-5633

[email us here](#)

Visit us on social media:

[LinkedIn](#)

[YouTube](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/942826440>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire,

Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.