Shumaker

DECEMBER 12, 2025 | PUBLICATION

"Offshoring Patient Data: What Health Care Providers Need to Know Now"

Health care providers are increasingly seeking creative ways to maintain profitability in the face of rising costs and reduced or stagnant reimbursement. Offshoring vendors for revenue cycle, information technology (IT), and other administrative functions is an attractive option that typically does not affect patient-facing workflows. The cost efficiencies are real, but so are the legal and compliance implications when patient information flows beyond U.S. borders. The rules are a patchwork of federal requirements, Medicare and Medicaid program guidance, and state specific restrictions, some of which categorically prohibit offshoring certain data. Providers that store or allow access to protected health information (PHI), as defined under the Health Insurance Portability and Accountability Act (HIPAA), should understand where the tripwires lie.

HIPAA and Federal Considerations

Surprisingly, HIPAA does not prohibit PHI from being accessed or stored outside the United States. Covered entities and business associates may use cloud, hosting, or service providers whose servers or personnel are offshore, provided they otherwise comply with HIPAA *writ large*. That means entering into a compliant business associate agreement (BAA), implementing reasonable and appropriate safeguards, and ensuring minimum necessary access. The practical challenge is enforcement and risk allocation. While HIPAA, as strengthened by the Health Information Technology for Economic and Clinical Health Act (HITECH), imposes

INDUSTRY SECTOR

Health Care
Technology

SERVICE LINE

Health Law
Technology, Data Privacy, Cybersecurity & AI

RELATED PROFESSIONALS

Grant P. Dearborn
Mara J. Rendina

MEDIA CONTACT

Wendy M. Byrne
wbyrne@shumaker.com

direct liability on business associates, regulators' ability to pursue offshore entities is limited. As a result, the covered entity often bears the brunt of breach response, remediation, and regulatory exposure if an offshore vendor mishandles PHI. These realities elevate the importance of due diligence, contractual protections, and verifiable controls.

For Medicare Advantage and Medicare Part D programs, the Centers for Medicare and Medicaid Services (CMS) has not banned offshoring but imposes additional oversight. Plans must obtain detailed attestations regarding any offshore subcontractors that "receive, process, transfer, handle, store, or access" beneficiary PHI, describing the offshore functions, PHI involved, and safeguards in place. Those obligations typically flow down to providers in network and downstream agreements, along with audit rights and reporting duties. Providers supporting Medicare Advantage operations should anticipate, and be prepared to demonstrate, offshore controls aligned with CMS expectations.

Medicaid Brings State by State Variability

At the federal level, Section 6505 of the Affordable Care Act (ACA) prohibits state Medicaid programs from paying for items or services furnished by entities located outside the United States. CMS clarified that this prohibition is aimed at benefits and services and does not target administrative support. States, however, are increasingly tightening the reins through policy manuals, procurement terms, and managed care contracts. Some prohibit any offshoring of Medicaid data outright; others require all work and data storage to remain within the U.S. Texas is a leading example: its Uniform Managed Care Contract prohibits performance of work or maintenance of information outside the United States and bars remote offshore access to Texas Health and Human Services systems or data. Other states impose similar restrictions via executive orders or programmatic rules, and some require prior approval or affirmative attestations before offshore resources may be used. In Ohio, gubernatorial executive orders prohibit executive agencies from contracting for services to be performed outside the United States and extend those limits to subcontractors. Those requirements typically flow through Medicaid procurements and managed care contracts. In Florida, beyond HIPAA, state law prohibits certain Florida-licensed providers using certified electronic health record (EHR) technology from storing qualified electronic health records outside the United States, its territories, or Canada; Medicaid participants operating in Florida must account for this localization mandate in their arrangements with plans and vendors. The upshot is that Medicaid-related offshoring is lawful in principle but often curtailed in practice by state-specific terms.

Practical Steps for Providers Considering Offshore Arrangements

A risk informed approach can enable compliant operations while avoiding regulatory surprises. Health care providers across the continuum of care should:

- Inventory data flows to identify whether any offshore personnel or infrastructure have access to or store PHI, including backup files and logs.
- Map payer and program exposure, because Medicare Advantage and Medicaid bring layered obligations and audit rights beyond HIPAA.
- Screen for state mandates and contract terms that prohibit or restrict offshoring, particularly for Medicaid managed care participants.
- Strengthen contracts to include minimum necessary access, encryption in transit and at rest, breach notification timelines, security certifications, audit and inspection rights, termination for cause, indemnities, and, where feasible, dispute resolution and enforcement mechanisms that have practical bite against offshore entities.
- Test and verify by conducting annual security and privacy audits of offshore subcontractors, validate Internet Protocol (IP) restrictions and access controls, and document remediation.

- Engage legal counsel with subject matter expertise to clarify applicable offshoring restrictions and advise on best practice processes and contract language aligned with identified goals and risk tolerance.

The regulatory environment is trending toward stricter localization and more robust cybersecurity expectations. Providers that proactively align the rules discussed herein, while imposing verifiable obligations on all downstream vendors, will be positioned to appropriately engage offshore vendors without compromising compliance.

If you would like more information on navigating federal and state restrictions on offshoring patient data, please contact Mara Rendina or Grant Dearborn.

Whether you are evaluating offshore vendors, strengthening contractual safeguards, or responding to evolving Medicare and Medicaid requirements, Shumaker's Health Law Service Line provides practical, experienced guidance to help you operate confidently and compliantly in a complex regulatory environment.

Shumaker