The Interoperability Trap: How TEFCA Design Choices Undermine Healthcar Equity for Cash-Pay Providers

MAY 09, 2025 • PAID

In the evolving landscape of healthcare interoperability, there has long been a pr —a vision that, through the judicious implementation of national frameworks ar trusted exchange networks, we would finally tear down the walls that have long isolated patient health data in proprietary silos. TEFCA, the Trusted Exchange Framework and Common Agreement, was heralded as a foundational step towar vision, bringing with it the hope of seamless, modern, patient-centric access to h records. Yet, in the very early stages of its implementation, an insidious contradi has emerged. While TEFCA promotes itself as a facilitator of equitable data acc current operationalization actively excludes a growing segment of healthcare providers: cash-pay clinics. These are not rogue operations or fringe entities. Th state-licensed, HIPAA-compliant, often digitally forward clinical practices that, many cases, offer superior patient engagement and continuity of care. And yet, t same clinics now find themselves shut out of the national networks they once accessed, not because they lack clinical legitimacy, but because they have opted the traditional insurance model.

This contradiction is not just philosophical; it is operational and profoundly damaging. Recently, I spoke with the leadership team of a primary care clinic tha structured itself around the principles of direct care. Their mission is simple: re administrative waste, offer transparent pricing, and prioritize the doctor-patient relationship over bureaucratic documentation. And yet, in a situation that shoul alarm any serious policymaker, this clinic was forced to delay care for an elderly patient because they could not receive her records in time. The hospital where sh recently been admitted, tethered to legacy workflows and suspicious of the clini

"non-traditional" payment model, failed to send the records electronically. Inste they were faxed—a method whose failure rate, latency, and lack of security is universally derided in the digital health space. Ironically, this clinic had been pa Health Information Exchange just a year prior. Their credentialing had not chan Their commitment to treatment and HIPAA compliance had not changed. What changed was the policy landscape—swept up in the aftermath of a single interoperability scandal and the reactive governance that followed.

To understand how we arrived at this impasse, one must look at the ripple effect what occurred between a data intermediary and one of the largest electronic hea record vendors in the country. The dispute began with the onboarding of certain entities to a national interoperability network under the guise of treatment-base access. While the technical definitions of treatment under HIPAA are relatively the application of those definitions, when filtered through the lens of risk aversi and competitive protectionism, can be interpreted far more narrowly. A handful onboarded organizations were found to be engaging in what appeared to be non- treatment activities, such as funneling patient data for mass tort legal actions. T data intermediary facilitating their access faced scrutiny, and rightly so. There is place for abuse in networks designed for clinical care. But the ensuing response dominant network stakeholders—particularly from those who control access to massive swaths of hospital and EHR data—was both sweeping and blunt. Rather targeting the misuse with scalpel-like precision, they wielded a hammer.

The result was the application of newly stringent Standard Operating Procedure SOPs, for vetting participants in interoperability frameworks. These SOPs, deve quickly and with limited transparency, redefined eligibility in ways that effectiv equated clinical legitimacy with insurance participation. The logic, if it can be c that, was straightforward: entities participating in insurance billing were easier track, and control. They left digital trails through claims data, could be reported fraud through payor relationships, and were generally part of the same ecosyster incentives that had long governed legacy healthcare institutions. Cash-pay provi by contrast, were harder to monitor through traditional mechanisms and thus, i eyes of SOP authors, posed a risk.

It is here that the fundamental philosophical flaw reveals itself. Healthcare interoperability was never meant to be a compliance mechanism for insurance infrastructure. It was not conceived as a tool to entrench existing business mode was designed to empower patients and providers—regardless of payment modali share, receive, and act upon health information in a way that improves outcomes reduces administrative friction. To now see this vision narrowed by gatekeeping criteria that are entirely financial in nature is to witness the perversion of the or goal.

The reality is that cash-pay providers are not inherently riskier. In fact, many di care clinics offer longer visits, lower patient panels, and tighter operational cont precisely because they are not beholden to the throughput demands of fee-for-se billing. These providers are often innovators in care delivery, leveraging digital t asynchronous communication, and personalized medicine models to better serve communities. Their exclusion from national networks is not only a disservice to patients—it is an institutional betrayal of the principles of clinical neutrality an access equity.

The problem is compounded by the opaque nature of how these SOPs were creat and who gets to enforce them. There is no public docket of stakeholders, no opportunity for comment or redress, no clear appeals process. The entities that maintain technical infrastructure for interoperability—be they Qualified Health Information Networks under TEFCA, or older frameworks like Carequality and CommonWell—are making access decisions that affect hundreds of thousands o providers and millions of patients. Yet these decisions are happening behind clo doors, with input from a limited circle of enterprise-focused participants. This l transparency breeds distrust and creates an uneven playing field where influenc integrity, determines access.

One of the great ironies in all of this is that the very actors the SOPs were desig exclude—fraudulent telehealth operators, shell clinics, and data brokers posing providers—can still often gain access simply by submitting the right insurance credentials. They may bill minimal amounts, use third-party credentialing servic operate out of virtual addresses, but so long as they exist on paper as part of the

traditional insurance system, they can slip through. Meanwhile, legitimate clinic with brick-and-mortar locations, robust clinical teams, and full HIPAA compliar are denied access because they have chosen to remove insurance from their operations. This is not risk management. It is risk misallocation.

A more sophisticated and fair approach would acknowledge the complexity of m care delivery and build fraud detection mechanisms that are behavior-based rath than status-based. Instead of assuming risk based on the presence or absence of insurance billing, networks should be analyzing query patterns, attestation quali and clinical documentation. They should deploy anomaly detection to flag unusu access behavior, implement graduated penalties for non-compliance, and create processes for remediation. None of this requires the exclusion of an entire class providers. It simply requires better tooling, better governance, and a willingness evolve past legacy heuristics.

At a deeper level, this debate touches on the role of interoperability in a system increasingly being shaped by alternative models of care. The rise of direct prima care, virtual-first care, behavioral health startups, and chronic care platforms ha introduced new operational structures that do not fit neatly into the mold of twentieth-century healthcare institutions. If interoperability is to be meaningful this new landscape, it must adapt to reflect the diversity of care models now serv patients. TEFCA's promise lies in its potential to standardize data exchange acro this diversity, not in its capacity to reinforce a narrow definition of provider legitimacy.

The policy path forward is clear, though not politically easy. First, there must be immediate effort to create an inclusion pathway for cash-pay providers that is ba on clinical credentials and compliance obligations, not financial arrangements. A provider with state licensure, an NPI, and demonstrable HIPAA compliance shou eligible to participate in treatment-based data exchange under TEFCA. This doe open the floodgates to abuse; it simply realigns eligibility with clinical reality. Se the governance structures that define SOPs and operational policies for interoperability networks must be democratized. Whether through public comm periods, advisory boards with diverse representation, or transparent publication

decision-making processes, the time has come to open the black box. Third, frau prevention must shift from gatekeeping to intelligent monitoring. Just as banks shut out all small businesses for fear of money laundering but instead monitor transactions for suspicious activity, interoperability networks must do the same data access.

TEFCA is still young. Its architecture is flexible enough to accommodate course corrections. But if it continues down its current trajectory, it risks becoming an enforcer of status quo healthcare power dynamics rather than a catalyst for patie empowerment and innovation. The goal should never have been to protect instit from innovation. It should have been to protect patients from information asymı administrative opacity, and the clinical dangers of fragmented care. Cash-pay providers are not a fringe group—they are a growing segment of the healthcare delivery landscape, one that is often closer to the patient, more responsive to cli nuance, and more willing to embrace new care paradigms. Excluding them from national health data conversation is not just policy malpractice. It is a strategic failure.

In the coming years, as TEFCA expands into use cases like Individual Access Ser and Public Health Reporting, the foundational decisions made today will reverb across every layer of our health system. If we cannot get the basic use case of treatment right—if we cannot ensure that any legitimate provider treating a pati can access the data needed to do so safely—then the rest is merely window dress is incumbent upon those shaping these frameworks to revisit their assumptions, broaden their perspectives, and return to the first principles of clinical care. Dat belongs to the patient. Providers serve the patient. And interoperability exists tc support that sacred relationship, not to constrain it through outdated proxies fo legitimacy.

The exclusion of cash-pay providers from national interoperability frameworks l TEFCA represents a form of systemic epistemic blindness, one that fails to comprehend the trajectory of healthcare delivery in the United States. What onc have been considered an outlier model—where patients pay directly for care, an providers structure their business models around clinical value rather than insu

billing—has now become a foundational pillar of primary and specialty care innovation. These clinics are often early adopters of new health technologies, electronic health record systems built for usability rather than compliance checl and care models that emphasize continuity over volume. Yet TEFCA's current implementation, rooted in the protective instincts of large institutional players, to recognize or accommodate this evolution.

What exacerbates the problem is that these exclusions are not based on clear evi of risk but on an assumption that insurance billing serves as a proxy for legitima This logic is dangerously flawed. Insurance billing does not guarantee that a pro is delivering high-quality care. It does not ensure ethical data usage, nor does it assurance against fraud. In fact, some of the most egregious instances of healthc fraud in recent history have occurred within the insured system, where phantom billing, upcoding, and patient data manipulation are not just possible—they are widespread. By contrast, many direct care providers operate in a transparent anc accountable manner precisely because their patients are their only source of reve and reputation.

The deeper issue is that the current framework for TEFCA, and by extension the broader interoperability regime, has not been built with adaptive governance in Governance in health IT tends to congeal quickly. Once a policy is set, particula one as foundational as eligibility criteria for network participation, it becomes difficult to unwind. The stakeholders involved—large EHR vendors, hospital sys and government agencies—often converge around risk-averse practices that favo incumbency and bureaucratic inertia. This is not because they are malicious. It i because they are accountable to large systems, complex risk portfolios, and compliance burdens that resist ambiguity. But in doing so, they build policy environments that are brittle, exclusionary, and ultimately unfit for a pluralistic healthcare economy.

To rectify this, a fundamental rethinking of interoperability governance is requi one that moves away from static credential-based exclusion toward dynamic, beh based inclusion. Imagine an interoperability framework where access is not determined by insurance contracts or billing codes but by adherence to transpar

clinical standards and observable behavior. Such a framework would allow for continuous monitoring of data access patterns, flagging anomalous behaviors tha deviate from expected clinical workflows.

This model of behavior-based access is not hypothetical. It draws from principle already in use in other sectors where sensitive data exchange occurs at scale. Cor the financial services industry, which processes trillions of dollars in daily transactions. Access to core banking APIs, international wire transfers, and real payment systems is not granted solely based on whether a business fits a traditio mold. It is granted through a blend of credential validation, transaction monitor and adaptive risk scoring. The notion that a provider must prove legitimacy by aligning with a legacy business model would be laughable in banking or logistics healthcare continues to conflate operational orthodoxy with trustworthiness.

If TEFCA is to fulfill its mission, it must integrate a similar logic. The first step doing so is to formalize the concept of continuous vetting. Rather than relying o one-time approval process or manual SOP-based screening, participation in nati networks should be governed by persistent verification, with real-time monitorir data use behaviors. This would allow the system to distinguish between providers make legitimate treatment-based queries and actors who seek to exploit the netv for purposes inconsistent with patient care. The metrics for such monitoring alr exist—query frequency, target diversity, response utilization, and even alignmen between query type and specialty can all serve as inputs into a risk profile. Wher unusual patterns are detected, a tiered escalation protocol can guide review, rath than triggering a punitive expulsion that penalizes providers for systemic design flaws.

A continuous vetting framework also allows for flexibility across care models. A volume mental health practice in a rural town will not behave like a high-acuity urgent care chain in an urban center. Nor should it have to. The system must be intelligent enough to understand these nuances. Risk is not a monolith, and neit legitimacy. By embracing variability rather than resisting it, TEFCA could creat framework that is resilient, adaptive, and inclusive—all without sacrificing secu compliance.

Yet none of this can occur unless the governance structures that oversee TEFCA made transparent and participatory. Currently, a small number of organizations an outsized role in determining who gains access and under what conditions. Th entities, while technically sophisticated and operationally necessary, do not repr the full spectrum of healthcare delivery. They are disproportionately staffed and influenced by stakeholders whose interests are aligned with institutional scale, reimbursement infrastructure, and network control. The voices of small practice virtual care providers, and cash-pay clinics are effectively absent from the rooms where these decisions are made.

This is a governance failure, not a technological one. TEFCA's governing bodies include seats for cash-pay clinics, virtual-first care providers, rural practitioners others operating outside the traditional healthcare establishment. These stakeh must not be token voices, but equal participants in the deliberative process that shapes national data exchange policy.

Furthermore, a formal appeals process should be established—one that allows d providers to present evidence of legitimacy, intent, and compliance. This proces should be handled by a neutral entity with the authority to override or modify decisions, ensuring that access is not arbitrarily denied. The appeals process sho also include published decisions with redacted details, to establish precedent an ensure accountability. Without such mechanisms, the onboarding process becon opaque, bureaucratic, and susceptible to institutional bias.

Another key component is building a technical monitoring infrastructure that c support proportional oversight. Instead of assuming bad faith and designing pol to exclude, TEFCA must assume good faith and verify it through intelligent aud mechanisms. These can include real-time query dashboards, machine learning m that detect anomalies, and collaborative review teams that include clinicians, da scientists, and compliance officers. When misuse is detected, sanctions should b proportionate—ranging from queries suspension to access revocation—but alwa transparent, appealable, and rooted in clinical and ethical analysis.

In the end, the health of any interoperability framework is measured not by the rigidity of its gates, but by the integrity of its flows. TEFCA was built to facilita trust, but trust is not a static credential. It is an ongoing process of transparency participation, and shared responsibility. When that process excludes entire categ of providers for failing to adhere to legacy economic models, it betrays the very concept it was meant to uphold.

We are standing at a critical juncture. The policies we implement today will defi shape of our data ecosystems for decades to come. Will they be open, adaptive, a patient-centered? Or will they become yet another mechanism through which entrenched power structures control access to the tools of modern care?

The future of healthcare will not be uniformly institutional. It will be pluralistic messy, dynamic, and decentralized. Our interoperability systems must reflect tha reality. If we fail to adapt, we will have built the infrastructure of yesterday for t patients of tomorrow. And in doing so, we will have squandered the rarest of opportunities: the chance to build a health data system worthy of the trust we sc claim to defend.

1 Like • 1 Restack

← Previous

Nex

Discussion about this post

Comments Restacks

Write a comment...