The Coming Audit Economy: How Epic Health Gorilla Could Birth a New Industry in Healthcare Data Complian

JAN 15, 2026 • PAID

Abstract

Epic Systems' January 2026 lawsuit against Health Gorilla and affiliated entities alleges systematic fraud in healthcare interoperability networks, claiming defen falsely asserted treatment purposes to access patient records that were then monetized for mass tort litigation. While these remain unproven allegations in a litigation, they expose potential structural vulnerabilities in TEFCA and Carequ frameworks that currently rely on trust and self-policing without systematic verification. If even a fraction of the alleged misconduct proves accurate, regulat response becomes likely. This analysis examines how such response might create demand for purpose-of-use auditing services analogous to Medicare Advantage r adjustment validation, explores what such a market could look like, and develop conceptual business case for technology-forward entrants. Market sizing and projections are necessarily speculative given the nascent nature of this potential opportunity.

What the Epic Complaint Actually Alleg

The January 13, 2026 complaint filed in Central District of California makes swe fraud allegations against multiple defendants. These are allegations in active litigation, not established facts. Defendants will present their own evidence and interpretations. That caveat is critical for everything that follows.

Epic alleges that Health Gorilla, operating as both a Carequality Implementer ar TEFCA QHIN, onboarded entities claiming treatment purposes for accessing pa records when their actual purposes were non-treatment commercial exploitation complaint names three primary defendant groups beyond Health Gorilla: Ravilla and affiliated entities, Mammoth and affiliated entities, and Unit 387 with its downstream connections.

According to the complaint, RavillaMed joined Carequality in August 2024 thro implementer Metriport, pulled 32 records, then was quickly removed after Metr grew suspicious. Health Gorilla then onboarded RavillaMed to both Carequality TEFCA in October 2024 despite this red flag being potentially visible. From Oct 2024 through December 2025, RavillaMed allegedly accessed over 42,000 patient records from Epic customers alone, claiming treatment purposes for all requests

The complaint alleges RavillaMed is closely connected to LlamaLab, a company openly markets same-day patient record retrieval for law firms. Evidence cited includes RavillaMed owner Dr. Avinash Ravilla being listed on LlamaLab's webs Chief Medical Officer, Ravilla's wife working as LlamaLab's Director of Medical Records, and LlamaLab CEO Shere Saidon participating in RavillaMed's technic onboarding meetings with implementers. The complaint characterizes returned documentation as clinically useless, organized by PFAS exposure markers releva litigation rather than treatment.

For Mammoth entities, the complaint alleges they accessed over 140,000 records Epic customers while returning blank or minimally useful clinical documentatic The complaint highlights connections to Daniel Baker, who the complaint notes pleaded guilty to federal conspiracy to defraud charges in 2014 in the Central D of California and was CEO of Integritort, which Carequality banned in October for non-treatment data access. The complaint alleges Baker co-founded Mammo and serves as CTO despite sworn statements from Mammoth CEO Ryan Hilton denying Baker's involvement.

Unit 387 and its downstream connections SelfRx and GuardDog allegedly show similar patterns. The complaint notes SelfRx went from single-digit monthly qu

to 17,000 in December 2024. GuardDog's authorized official also founded Mass T Medical Consultants. Unit 387's CEO Meredith Manak also founded Hoppr, whi markets instant patient record access to law firms and insurance companies.

The complaint presents exchange pattern data showing non-reciprocal flows wh defendants pulled far more records than they returned, volume spikes inconsiste with normal treatment patterns, and returned documentation lacking clinical co These patterns allegedly indicate non-treatment purposes despite treatment attestations.

Health Gorilla allegedly failed to adequately vet these connections before onboa and defended them when Epic raised concerns rather than investigating. When presented with evidence of problems, Health Gorilla allegedly provided explanat Epic characterizes as false, such as claiming record spikes were technical glitche causing duplicate requests.

Again, these are allegations. Health Gorilla and the other defendants will disput these characterizations. They may present evidence showing their connections d provide legitimate treatment, that exchange patterns have innocent explanations that documentation Epic characterizes as junk actually reflects valid clinical pra Sworn statements from defendants denying misconduct suggest vigorous defens coming. The litigation will take years to resolve.

Why Trust-Based Systems Fail Without Verification

Setting aside whether Epic's specific allegations prove accurate, the complaint highlights a structural governance question in healthcare interoperability. Both TEFCA and Carequality operate on distributed trust models where implemente QHINs vet their connections, and framework operators provide governance infrastructure but don't independently verify each participant.

This approach has legitimate rationale. Carequality has over 100,000 connection hundreds of changes daily. TEFCA is growing toward similar scale. Central

verification of every participant and every query would be operationally impossi and prohibitively expensive. The frameworks instead establish contractual obligations, require implementers to flow down these obligations to connections provide dispute resolution when problems arise.

But this creates obvious misaligned incentives. Implementers and QHINs genera revenue from connections and transaction volumes. Every additional connection means more revenue. Thorough vetting costs money and delays revenue generati Removing problematic connections after onboarding reduces revenue. Absent ex pressure, the rational economic choice is minimal vetting and maximum toleran questionable connections.

Framework operators like Carequality and TEFCA's RCE face resource constrai Carequality is administered by the Sequoia Project with limited staff managing massive connection populations. Systematic audit of participant behavior isn't w their operational model or budget. TEFCA similarly relies on QHINs to police t own participants.

Participating providers lack real-time fraud detection capability. When a query arrives asserting treatment purpose, EHR systems automatically respond withou human review. Providers might notice suspicious patterns retrospectively if they analyze logs, but most lack resources for such analysis. Even Epic, with significa technical sophistication, relied on customer complaints to initially flag concerns before conducting deeper analysis.

This combination creates what economists call a market failure. The parties bes positioned to prevent fraud have minimal incentive to do so. The parties harmed fraud have limited detection capability. Framework operators lack resources for systematic policing. Bad actors can exploit these gaps if willing to lie about purp

Whether the exploitation is as widespread as Epic alleges remains to be proven. the structural vulnerabilities exist regardless. Even if Epic's specific defendants innocent, the framework design creates opportunities for future bad actors. Som

level of systematic verification beyond self-attestation seems necessary for long-t framework viability.

The RADV Precedent and Its Applicabil

Medicare Advantage risk adjustment validation provides a precedent for how regulators address systematic gaming in healthcare payment and data systems. Understanding RADV helps predict potential approaches to purpose-of-use verification, though important differences exist.

Medicare Advantage plans receive capitated payments adjusted for patient risk. enrolling sicker patients get higher per-member-per-month payments. This crea incentives to document more conditions regardless of whether they affect care o treatment. Early Medicare Advantage history showed rapid risk score inflation a plans optimized coding.

CMS responded with RADV audits where contracted private firms review medic records to verify that reported diagnoses have supporting documentation. The a sample enrollees, require plans to produce records, and extrapolate findings to payment adjustments. This approach balances thoroughness with practical cons on reviewing every diagnosis for every patient.

The RADV audit industry now includes multiple large contractors plus ancillary services like audit preparation consulting, appeal representation, and coding optimization platforms. While exact industry size is difficult to pin down witho access to all CMS contracts and private market consulting fees, the audit infrastructure is substantial enough to support several large contractors and numerous specialized service providers.

Several RADV characteristics could translate to purpose-of-use auditing. First, t audit function gets outsourced to private contractors rather than performed by government directly. Second, audits focus on verifying claims match supporting evidence rather than second-guessing clinical judgment. Third, sampling enable

coverage without reviewing every transaction. Fourth, the audit creates an ecosy of adjacent services beyond basic audit work.

But important differences exist between RADV and potential purpose-of-use au RADV addresses financial fraud with clear dollar amounts at stake and straightforward remedies through payment adjustments. Purpose-of-use violatic involve privacy harms and contractual breaches that are harder to quantify and remedy. RADV audits medical records to verify diagnoses were documented. Pu of-use audits would need to determine whether requestors actually provided treatment, which is more complex than checking documentation exists.

RADV also operates in mature Medicare Advantage markets with established populations and stable payment flows. Purpose-of-use auditing would address emerging interoperability frameworks still gaining adoption. The regulatory environment differs too, with CMS having clear statutory authority over Medica Advantage while TEFCA governance relies on contract rather than direct regula mandate.

Despite these differences, the RADV model demonstrates that systematic audit healthcare data claims is feasible, that private contractors can effectively perfor such audits at scale, and that audit markets can sustain multiple large players pl surrounding ecosystems. If regulators determine that purpose-of-use verificatio needs systematic auditing, RADV provides a template for implementation.

Potential Regulatory Responses and Their Probability

The Epic litigation will likely catalyze some regulatory response, though the for timing remain uncertain. Several scenarios have different probability levels base political dynamics, agency priorities, and litigation outcomes.

High probability responses, perhaps 60 to 70 percent likely within 24 months, ir enhanced framework governance requirements without mandated third-party au HHS and ONC could strengthen TEFCA rules requiring QHINs to implement s

verification practices at onboarding and ongoing monitoring. This might include requiring clinical site visits, reference checks, review of sample queries, and documented policies for investigating suspicious patterns. Carequality might ad similar enhanced standards voluntarily or under pressure from implementers concerned about liability. This response is likely because it requires no addition federal funding, can be implemented through rulemaking or framework policy updates, and addresses concerns without creating new bureaucracy.

Increased HIPAA enforcement around false pretenses is also highly probable. Th existing criminal prohibition at 42 USC 1320d-6 already covers obtaining record under false pretenses with intent to sell. OCR could signal increased enforceme priority and pursue civil penalties against entities whose purposes don't match attestations. This requires no new statutory authority and sends strong deterren signals. Probability is high because it's within existing agency discretion and res to demonstrated problems.

Framework transparency requirements would mandate that framework operator publicly report aggregate statistics on dispute resolution, suspended participant identified violations. This increases accountability without requiring audits. Probability is moderate to high because transparency is politically popular and operationally simple.

Moderate probability responses, perhaps 30 to 50 percent likely within 36 montl include mandatory audit requirements similar to RADV. HHS could promulgate requiring periodic audits of TEFCA participants exceeding specified query thresholds, with audits conducted by contracted private firms. This would creat market opportunity discussed throughout this analysis. Probability is moderate than high because it requires significant rulemaking process, budget implicatio contracting audit services, and political will to create new oversight mechanisms probability increases substantially if Epic litigation reveals fraud more widespre than currently alleged or if additional scandals emerge.

Background check requirements could mandate criminal background checks an professional licensing verification for entity owners and key personnel before

framework access is granted. This would have prevented someone with Daniel B background from controlling entities with patient data access. Probability is mo because it's straightforward to implement but faces potential pushback on cost a potentially discriminatory against individuals with criminal records seeking rehabilitation.

Technical controls mandating reciprocal documentation could require entities claiming treatment purposes to return clinical documentation for some percenta queries, with failure triggering automatic suspension. This creates technical verification without human audit. Probability is moderate because it's technicall feasible but might impose burden on legitimate users and could be gamed throu junk documentation.

Lower probability responses, perhaps 10 to 30 percent likely, include Congressi legislation creating new statutory framework. Congress could amend the Cures explicitly require verification mechanisms with civil penalties for implementers failing to adequately vet connections. Probability is low because healthcare legis faces partisan gridlock and this issue likely lacks salience for most members. Probability increases if the issue gains significant media attention or affects influential constituencies.

Creation of federal audit office where HHS establishes a dedicated office for healthcare interoperability oversight with staff conducting audits directly rathe contracting them out has low probability because it requires substantial budget appropriations and expansion of federal workforce, both politically challenging.

State-level regulatory patchwork where individual states impose their own audit verification requirements for entities accessing their residents' data has moderat probability for a few states like California and New York with strong privacy lav low for comprehensive national patchwork. This scenario creates complexity wit necessarily addressing the problem effectively.

Litigation outcomes matter significantly. If Epic obtains substantial judgments a the evidence reveals widespread fraud, regulatory response intensifies. If defend

prevail or the case settles quietly, urgency diminishes. Discovery will be particul important. If depositions and documents show egregious misconduct, public pre for response increases. If evidence is ambiguous, regulators might take wait-and approaches.

Additional scandals would accelerate response. If journalists or other providers identify more bad actors exploiting frameworks, the cumulative effect forces act One lawsuit might be treated as isolated incident. Multiple revelations suggest systemic problems requiring systematic solutions.

Political dynamics affect probability and timing. An administration focused on healthcare regulation might pursue aggressive responses. Different political leadership might favor lighter-touch approaches. Budget constraints affect feasi of audit mandates requiring federal contracting.

Framework operator response influences regulatory calculus. If Carequality and TEFCA implement meaningful reforms proactively, regulators might decide self governance is working adequately. If frameworks resist changes or implement cosmetic reforms, regulatory mandates become more likely.

The most probable scenario combines enhanced governance requirements with increased existing-authority enforcement and modest transparency mandates, stopping short of comprehensive audit requirements in the near term. This addr immediate concerns while preserving flexibility and avoiding commitment to on audit infrastructure before understanding the problem's true scope.

Conceptual Market Sizing with Transparent Assumptions

Estimating potential market size for purpose-of-use auditing requires stacking multiple assumptions. The following analysis shows the reasoning while acknowledging significant uncertainty at every step.

TEFCA reportedly had approximately 1,000 participants as of early 2026 per the complaint. Growth projections are speculative but might reach 3,000 to 5,000 participants by 2028 and possibly 10,000 by 2030 if adoption accelerates. These projections assume TEFCA achieves critical mass as the federal framework but c be too optimistic if adoption stalls or too conservative if policy changes accelera uptake.

Carequality has over 100,000 connections currently per the complaint. However, are individual practices with minimal query activity. Perhaps 10,000 connections conduct significant volumes warranting audit attention. This number might gro 25,000 as more entities recognize data access value and barriers to entry remain

Assume regulatory response requires annual audits of participants exceeding 1,0 queries annually. This threshold captures systematic data accessors while exemp small practices making occasional queries. Under this assumption, perhaps 30 to percent of total participants face mandatory annual audits by 2028. This yields approximately 1,500 TEFCA participants and 7,500 Carequality connections sub to audit, totaling 9,000 entities.

This assumption could be dramatically wrong. Regulators might set much highe thresholds like 10,000 or 50,000 queries, reducing audited populations by 80 to 9 percent. Or they might set lower thresholds or audit all participants regardless o volume, increasing populations substantially. The 1,000 query threshold is a gue regulatory balancing of thoroughness versus burden.

Pricing depends heavily on audit scope and participant size. Hypothetical pricin might include small participants with 1,000 to 10,000 queries paying perhaps 50 to 75,000 for basic audits reviewing 100 to 200 sampled queries with correspond clinical documentation. This assumes perhaps 80 hours of clinical reviewer time loaded costs of 400 dollars per hour plus project management and reporting. Me participants with 10,000 to 100,000 queries might pay 150,000 to 250,000 for expanded sampling and more detailed analysis, maybe 250 hours of clinical revie plus analytics. Large participants with over 100,000 queries might pay 400,000 t

800,000 for comprehensive audits with large sample sizes and detailed pattern analysis.

Using a blended average of 120,000 per audit across the population, 9,000 annua audits would generate approximately 1.1 billion in direct audit services revenue.

These pricing assumptions could be off by 50 percent or more. Actual audit cost depend on methodology, clinical reviewer wages, technology leverage, competiti dynamics, and regulatory specifications. Early audits might cost more as methodologies are established. Later audits could cost less with automation and learning effects. Or they could cost more if requirements expand based on initia findings.

The RADV precedent suggests adjacent services could generate revenue compar to direct audits. Pre-audit preparation consulting where half of audited entities purchase preparation services at average 40,000 yields 180 million annually. This assumes entities find value in advance preparation to reduce findings risk. Audit response and appeals where 20 percent of audits generate findings requiring res and average response costs are 120,000 adds 216 million annually. Continuous monitoring platforms where 40 percent of at-risk entities purchase SaaS monito average 35,000 annually adds 126 million. Training, certification, and other servi perhaps contribute 80 million annually across various categories.

Total adjacent services might reach 600 million annually, bringing total market t approximately 1.7 billion. By 2030, with participant growth and market maturat the total might reach 2.5 to 3 billion annually across direct audits and adjacent services. International expansion as other countries develop similar frameworks add another 500 million to 1 billion.

These estimates have enormous error bars. The true market could be 75 percent smaller or 200 percent larger depending on actual regulatory requirements, participant populations, competitive pricing, and scope definitions. Key variable highest uncertainty include whether audits get mandated at all versus other regulatory approaches, query volume thresholds for audit requirements, actual

participant population growth rates, competitive dynamics affecting pricing, technology leverage reducing audit costs, and scope of what audits must examin

A conservative scenario with high query thresholds, slow TEFCA adoption, and technology leverage might yield 500 to 800 million total market. An aggressive scenario with comprehensive audit requirements, rapid framework growth, and manual-intensive audits could reach 4 to 5 billion.

These estimates can be pressure-tested against other healthcare audit and compl markets. Healthcare compliance consulting across all functions likely exceeds 5 billion annually. RADV audit spending is probably in the range of 200 to 400 mi annually based on CMS contract announcements and known contractor activity, though precise figures aren't publicly available. Medical coding audit and educa markets are several hundred million annually.

A purpose-of-use audit market reaching 2 to 3 billion would represent a meanin new segment but not an implausibly large one given the underlying participant population and the importance of the data being protected. It would be smaller major healthcare IT markets like EHR systems, revenue cycle management, or population health but comparable to specialized segments like medication adhe platforms or care coordination software.

What a Purpose-Built Audit Company Might Look Like

If the regulatory scenario unfolds and audit demand materializes, what characte would successful entrants need? This section develops a profile of a hypothetica company, call it VerifyHealth, to illustrate the key capabilities and strategic cho

VerifyHealth would need to combine several expertise domains rarely found tog Healthcare domain knowledge is essential for understanding clinical workflows, documentation standards, and appropriate treatment coordination patterns. Tec sophistication is required to ingest and analyze large-scale transaction logs, buil pattern detection algorithms, and integrate with diverse health IT systems. Audi

methodology expertise ensures systematic sampling, evidence review, findings documentation, and quality assurance meeting regulatory standards. Regulatory relationships provide credibility with HHS, ONC, state agencies, and framework operators.

No existing company category perfectly combines these requirements. Tradition healthcare audit firms conducting RADV audits have clinical review and audit methodology but often lack deep technical capabilities for analyzing interoperab protocols. Health IT analytics companies have data engineering and EHR expert but lack audit rigor and regulatory relationships. Major consulting firms have government contracting experience but struggle with competitive pricing given overhead structures. Cybersecurity firms have technical investigation skills but l clinical capabilities.

This capability gap creates opportunity for purpose-built entrants or creative combinations through partnerships and acquisitions. VerifyHealth might emerg through several paths. A health IT analytics company could acquire a smaller me record review firm for clinical capacity while building out audit methodology th strategic hires from RADV contractors. This combines technical and clinical capabilities while adding audit expertise. A healthcare audit firm might partner health IT vendor to access technical infrastructure and integration capabilities v the audit firm provides methodology and regulatory relationships. Partnership r than acquisition preserves each company's core business while enabling collabor

A new venture could assemble the hybrid team from scratch through strategic h Recruit a founding team combining healthcare audit veterans, health IT product managers from EHR vendors or HIEs, clinical experts with relevant specialties, a data scientists. This avoids legacy systems and cultural integration challenges bu requires longer ramp to credibility. Private equity could back a roll-up strategy v multiple smaller capabilities get acquired and integrated. Buy a medical record company for clinical reviewers, a health IT consulting firm for technical integrat and an audit services firm for methodology, then integrate them under unified management.

The technology architecture would be cloud-native from inception, built to hanc massive data volumes and rapid scaling. Core components would include automa data ingestion pipelines supporting multiple formats, entity intelligence databas aggregating information from transaction logs and external sources, machine lea models detecting anomalous patterns, clinical documentation review platforms v structured workflows, and evidence synthesis engines producing regulatory com reports.

Critical make-versus-buy decisions shape the business model. Should VerifyHea build clinical review capacity internally or partner with medical record review companies that supply trained clinical staff? Should integrations with EHR vend developed in-house or licensed from HIE platforms? Should the company focus exclusively on audit services or expand vertically into preparation consulting, monitoring platforms, and response services?

Early strategic choices create path dependencies. A company positioning as prer quality auditor with high pricing builds different capabilities than one pursuing volume-based competitive pricing. Geographic expansion decisions matter, with first focus differing from designs supporting international markets. Partnership intensity with framework operators could range from arm's length contractor relationships to deep collaboration shaping audit standards.

Several moat-building strategies could create defensible positioning. Early regul approval of methodology makes later entrants justify why their approaches are superior. Accumulating audit data creates network effects as pattern detection improves with each audit. Building large clinical review workforces takes time competitors cannot instantly replicate. Technical integrations with major EHR vendors create switching costs. Brand reputation for audit credibility builds slo through consistent quality.

Technical Architecture for Hypothetical Validation Platform

A purpose-of-use validation platform would need sophisticated architecture addressing data ingestion, pattern analysis, documentation review, and evidence synthesis at scale. This section outlines a conceptual technical design.

The data ingestion layer would receive transaction logs from QHINs, implement and participants in various formats including HL7 FHIR bundles, X12 logs, SAM tokens, and IHE XDS.b metadata. Streaming architecture using Kafka handles re time feeds with schema validation ensuring quality. Failed validations route to exception handling. Successfully ingested data lands in partitioned data lake sto enabling efficient querying.

An entity intelligence database maintains comprehensive profiles for all entities profile includes identifying information, clinical service descriptions, behavioral metrics tracking query patterns, and network relationship maps. The database in feeds from NPI registries, state licensing databases, framework directories, publ filings, and web scraping. This aggregation creates holistic entity views supporti risk assessment.

The pattern detection engine applies machine learning to identify anomalous behaviors. Models detect volume anomalies using time series analysis, reciprocit imbalances through graph analysis, geographic anomalies comparing query locat to service areas, demographic targeting identifying populations queried at unusu rates, and document quality issues through natural language processing. The eng generates risk scores prioritizing entities for manual audit.

Clinical documentation review platforms provide trained auditors with structur workflows. For sampled queries, the platform retrieves requests, responses, and returned documentation. Auditors assess consistency with stated purposes using standardized coding schemes. Decision support tools flag documentation anoma like missing elements or stock language. Quality assurance functionality enables inter-rater reliability testing to ensure consistent application of standards.

Evidence synthesis engines aggregate findings into entity-level conclusions. Stat methods extrapolate sample findings to full populations with confidence interva

Multiple reporting formats serve different audiences: regulatory reports followi mandated templates, entity reports detailing findings with supporting evidence, aggregate dashboards showing patterns across populations.

Security architecture follows HITRUST, HIPAA, and SOC 2 requirements given sensitivity of patient data. Role-based access controls limit exposure. Comprehe audit trails log all data access. Encryption protects data throughout. Multi-regio deployment ensures availability. The platform documents itself to support its ov regulatory audit.

Integration layers connect to external systems. APIs enable direct submission ra than manual transfers. EHR integrations automate clinical documentation extra Framework directory connections provide real-time updates. The architecture supports multi-tenancy for concurrent audits across jurisdictions with appropri isolation.

This technical vision requires substantial investment. Initial platform developm might need 12 to 18 months with a team of 15 to 25 engineers covering backend, engineering, machine learning, frontend, and DevOps. Costs could reach 5 to 8 million before generating revenue. Ongoing enhancement and scaling adds milli annually.

Technology choices matter strategically. Cloud platforms like AWS or Azure pro necessary scale but create vendor dependencies. Open-source components reduc licensing costs but require maintenance overhead. Build-versus-buy decisions fo component affect time to market and long-term flexibility.

Business Model Possibilities and Rever Scenarios

A purpose-of-use audit company could pursue several revenue models with diffe characteristics.

Direct audit services fees charged per audit engagement would scale pricing wit participant size. Revenue is project-based and potentially lumpy, with spikes du audit cycles. Margins depend on operational efficiency but could reach 20 to 30 percent at scale for specialized services. Government contracts through HHS or framework operators might use different structures like per-participant pricing volume discounts.

Continuous monitoring subscriptions offering SaaS platforms for real-time risk assessment would have tiered pricing based on query volumes, perhaps 10,000 to 250,000 annually depending on participant size. This revenue is recurring and predictable, providing stable cash flow. Customer acquisition costs are moderate Churn should be low given switching costs. Margins could exceed 70 percent aft platform development.

Pre-audit preparation services help participants ready themselves for upcoming audits. Engagements are short-term, perhaps 1 to 3 months, with pricing at 25,0 150,000 depending on scope. Revenue occurs episodically when audits are annou Margins are high since work leverages existing methodology.

Audit response and appeals services provide representation when findings emer Pricing could be hourly at 300 to 500 for senior staff or fixed-fee. Complex cases might require 100,000 to 250,000. This revenue is unpredictable but highly prof given specialized expertise required.

Training and certification generates revenue from courses, enterprise training contracts, and certification fees. Individual courses might be priced at 500 to 2,0 enterprise programs at 50,000 to 100,000, annual certification at 250 to 500. Rev is modest initially but grows as the compliance function matures.

Technology licensing provides platform access to implementers wanting to cond internal monitoring. Annual licenses might be priced at 200,000 to 500,000 depe on scale. Margins are high given minimal incremental delivery cost.

The revenue mix would evolve. Early years are audit-heavy establishing market presence. Middle years see monitoring subscriptions grow to 30 to 40 percent of

revenue as SaaS gains traction. Mature state might show balanced distribution: 4
percent audit services, 30 percent monitoring, 20 percent preparation and respo
10 percent training and licensing.

Hypothetical revenue trajectories might follow this pattern. Year 1 shows 3 to 6
million from initial pilot audits and early monitoring customers. Year 2 reaches
25 million as first regulatory contracts begin and monitoring scales. Year 3 achie
50 to 80 million with full audit cycles and several hundred monitoring subscribe
Year 4 reaches 120 to 180 million at significant market penetration. Year 5 achie
250 to 350 million approaching market leadership.

These projections assume capturing 15 to 20 percent audit market share and 25
percent monitoring subscriptions by year five. They also assume the regulatory
scenario actually materializes, which remains uncertain.

Profitability requires navigating heavy upfront investment against delayed reven
Years 1 to 2 likely show losses as platform development and methodology
establishment consume resources. Year 3 might reach breakeven as revenue scal
Years 4 to 5 could achieve 20 to 25 percent EBITDA margins as platform leverag
increases.

Capital requirements depend on growth strategy. Conservative estimates sugges
35 million in funding through profitability supports team building, platform
development, regulatory engagement, and early marketing. More aggressive stra
might need 50 to 70 million.

Go-to-Market Challenges in an Uncerta Market

Marketing and selling purpose-of-use audit services faces unusual challenges gi
market nascency and regulatory uncertainty. Potential customers often don’t yet
understand they have a problem needing solution.

The federal regulatory customer represents the largest potential opportunity bu longest sales cycle. HHS, ONC, and TEFCA's RCE might contract for audit servi mandates emerge. Reaching these buyers requires government contracting exper including GSA schedules, SAM registration, and relationships with key agency personnel. The sales cycle could span 18 to 24 months from initial engagement t contract award. But winning could yield 50 to 200 million over multi-year terms

Early engagement focuses on thought leadership and methodology development. Publishing white papers on verification approaches, presenting at government conferences, and participating in advisory groups builds credibility. When RFPs emerge, established expertise creates advantages. The risk is investing heavily in government relationships when mandates might not materialize.

QHINs and implementers have direct interest in demonstrating compliance and mitigating liability post-Epic litigation. But they're also price-sensitive since pas audit costs to participants is challenging. The value proposition emphasizes risk mitigation and competitive differentiation. Voluntary audits show good faith compliance efforts potentially reducing liability. Marketing strong oversight pra differentiates in competitive markets.

Healthcare providers and systems want assurance their data isn't being exploited Large health systems participating in frameworks are logical customers for monitoring and preparation services. But selling requires long cycles through committee-based buying. Value propositions focus on patient trust and data stewardship. The Epic plaintiffs demonstrated providers do care about these issu The challenge is translating concern into purchase decisions.

Content marketing addressing education gaps precedes direct sales. White pape webinars, blog posts, and case studies teach the market about purpose-of-use ris and solutions. This positions the company as a subject matter expert and genera inbound leads. Public relations around litigation and regulatory developments maintains visibility.

The fundamental challenge is market timing uncertainty. Investing aggressively capability building before demand materializes risks capital. Waiting for clear demand risks competitors capturing first-mover advantages. Threading this nee requires staged investment calibrated to regulatory signals and market feedback

Why This Opportunity Might Not Materialize

Intellectual honesty requires acknowledging this entire analysis could be wrong. Several scenarios would prevent the hypothesized audit market from developing

The Epic litigation might reveal less fraud than alleged. If discovery shows defe actually provided legitimate treatment or that exchange patterns have innocent explanations, concerns about systematic exploitation diminish. One lawsuit with questionable allegations doesn't justify building entire regulatory infrastructure

Regulatory response might take different forms than audits. Instead of mandatir third-party audits, HHS could strengthen technical controls like requiring recip documentation or implementing automated pattern detection at the framework Technology solutions might address concerns more efficiently than manual audi

Framework operators might implement effective self-governance making externa audits unnecessary. If Carequality and TEFCA adopt rigorous vetting standards, ongoing monitoring, and transparent enforcement, regulators might conclude se governance works adequately. The current system's perceived failures could be corrected through enhanced policies rather than external audit mandates.

Political and budgetary constraints might prevent audit mandates. Comprehensi audit programs require funding for contractor payments. In constrained fiscal environments, new spending programs face high bars. Without statutory manda and appropriations, HHS might lack resources to implement systematic auditing

The interoperability frameworks themselves might fail to achieve critical mass. I TEFCA adoption stalls and Carequality growth plateaus, the participant popula

never reach scales justifying elaborate audit infrastructure. Concerns about exploitation might actually slow framework adoption, creating a vicious cycle.

Market economics might not support viable audit businesses. If regulatory requirements are vague, competitive dynamics drive pricing very low, and audit is narrow, the market might generate insufficient revenue to sustain specialized providers. Generic consulting firms might perform perfunctory audits meeting minimum requirements without creating substantial market opportunity.

Alternative business models might better address the underlying problems. Inst after-the-fact auditing, innovation might come from technology platforms enabl real-time purpose verification, insurance products covering exploitation risks, o decentralized governance structures replacing current frameworks.

Technology leverage might make auditing so inexpensive that it doesn't require specialized companies. If machine learning models can reliably detect purpose-c violations from pattern analysis alone without manual clinical review, the audit function becomes a commodity that framework operators handle internally.

These counterarguments suggest caution about treating audit market emergence inevitable. The opportunity is highly contingent on regulatory choices, litigation outcomes, and market dynamics that could evolve very differently than projected

The prudent entrepreneurial approach treats this as an option to monitor rather a certain opportunity to pursue immediately. Watch the Epic litigation through discovery and early motions. Track regulatory signals from HHS and ONC. Obse framework operator responses. Develop technical prototypes and methodology frameworks that could be activated quickly if demand emerges. But avoid massi capital commitment until market formation becomes clearer.

For investors, this represents a wait and see opportunity where tracking costs ar but premature commitment risks significant capital. For existing companies in adjacent spaces, developing lightweight capabilities that could expand if needed provides optionality without distraction. For entrepreneurs, the calculus depend risk tolerance and alternative opportunities. The potential upside is substantial

market materializes as hypothesized, but probability-adjusted expected value re careful assessment given execution risk and market uncertainty.

The Epic v Health Gorilla litigation will serve as a forcing function clarifying wh systematic purpose-of-use fraud is real, whether existing governance is adequate whether regulatory intervention is coming. Until those questions resolve, the au economy remains a possibility rather than a certainty, deserving attention but nc uncritical acceptance.

1 Like • 1 Restack

← Previous

Nex

Discussion about this post

Comments Restacks

Write a comment...