

PRACTITIONER'S GUIDE

The Hidden Economics of Credentialing

A Framework for
Operational Redesign

Joey Costa | Provider Peak

Co-published with  Verifiable

Contents

TLDR	Measuring What Credentialing is Actually Costing You
Before Your Read	Credentialing Operations Self-Assessment Cheat Sheet
Framing	Who This Is Written For

Part 01 Understanding the Problem

Section 1

What Credentialing
Actually Costs

Section 2

Why the Process Has
Stayed Manual

Section 3

The Regulatory Acceleration —
Why "Wait and See" Has a Cost

Part 02 Measure Your Baseline

Section 4

Measuring Your Current State —
A Credentialing Maturity Framework

Section 5

The Ghost Network Problem —
Measuring What You Don't Know

Part 03 Making the Decision

Section 6

Choosing an Operational Model
— A Decision Framework

Section 7

Building the Internal
Business Case

Section 8

What to Look For When
Evaluating Technology

Part 04 Implementation

Section 9

Structuring a 90-Day Pilot

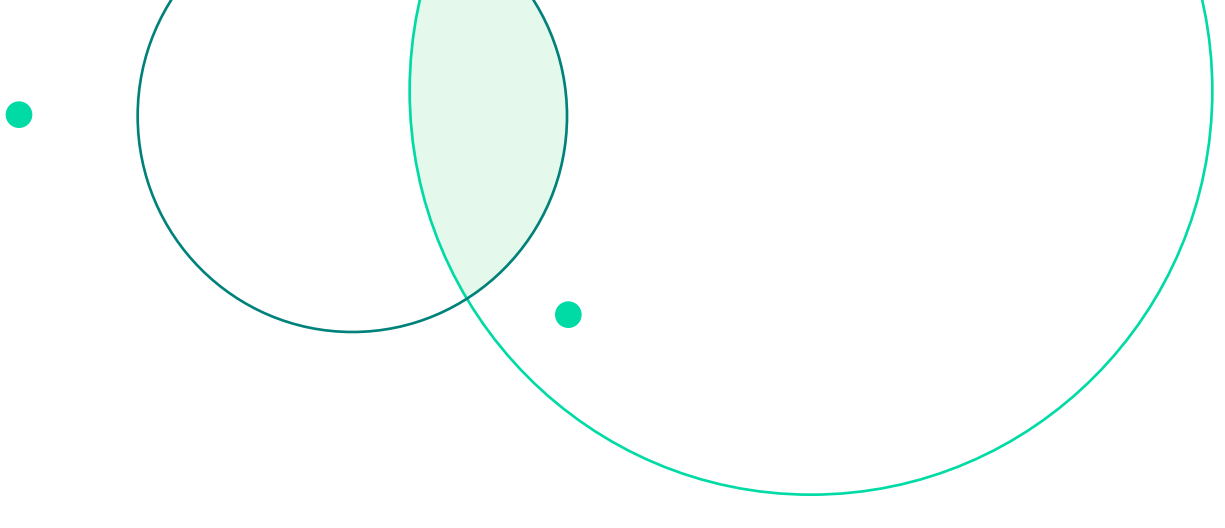
Conclusion

Structuring a 90-Day Pilot

About The Author Joey Costa · Provider Peak

About The Co-Publisher Verifiable





TLDR

Credentialing is a network growth constraint. Most health plans have never measured what it's actually costing them.

This paper gives payer network and operations leaders a diagnostic framework for measuring what slow credentialing costs, in days of delayed network access, dollars of vendor spend, and regulatory exposure. Then it provides a practical structure for making better decisions about technology, operational models, and vendor relationships. Whether you are managing a CVO contract, evaluating insourcing, or building the case for automation, the tools here apply regardless of your current situation or what path you take forward.



Tools you'll have access to

A cost framework you can use now

Five cost dimensions with calculation formulas, including network access delay cost and cost per credential, which most organizations have never formally measured.

[See Section 1](#)



A maturity framework for self-assessment

Score your operations across five dimensions before any vendor evaluation begins. Tells you what you're solving for, which determines what you should be evaluating.

[See Section 4](#)



A vendor-agnostic decision framework

In-house, outsourced, hybrid: a decision matrix based on growth urgency and current operational model, with ROI logic for each quadrant.

[See Section 6](#)



An internal business case structure

CFO, CIO, and COO translation frames. Seven KPIs defined before any pilot begins. Language your executive team will recognize.

[See Section 7](#)



A 90-day pilot structure

Phased design built for AI governance committees: non-clinical, parallel-run, KPI-defined before day one. Risk-profitable for risk-averse technology leaders.

[See Section 9](#)



A regulatory briefing in plain language

NCQA 2025, MHPAEA, CMS directory accuracy, No Surprises Act, and MA Star Ratings, mapped to what each requires of your current infrastructure.

[See Section 3](#)



Credentialing Operations Self-Assessment Cheat Sheet

Not interested in reading this entire whitepaper? Use this cheat sheet to determine how urgent your organization's need for credentialing transformation is. Five questions, one per maturity dimension, to locate your organization before reading. The lower your scores, the more urgent the regulatory and operational content ahead.

01.

Verification Completeness

What percentage of provider verifications return results automatically, without a coordinator making a manual call, submitting a web form, or logging into a portal?

- ☐ A Less than 40% — most verifications still require manual outreach
- ☐ B 40–70% — some sources automated, others still manual
- ☐ C 70–90% — most automated; some protected sources require intervention
- ☐ D 90%+ — near-complete automation including CAPTCHA-protected sources

02.

Monitoring Frequency

If a provider in your network received a new OIG exclusion today, how quickly would your system surface that information?

- ☐ A At the next re-credentialing cycle — months or years away
- ☐ B Within 30 days — monthly monitoring batch
- ☐ C Within 7 days — weekly scans
- ☐ D Within 24–48 hours — continuous or near-real-time monitoring



03.

**Data
Governance
Integrity**

Is your credentialing system the authoritative source of truth for provider status — or do the directory, claims, and enrollment systems maintain independent records?

- ☐ A No — each system has its own version; manual reconciliation required
- ☐ B Partially — credentialing is primary but directory diverges between cycles
- ☐ C Mostly — automated feeds keep systems in sync with occasional lag
- ☐ D Yes — single source of truth; status changes propagate automatically

04.

**Process
Auditability**

If a regulator asked today for the full verification history for a specific provider as of 18 months ago, how long would that take?

- ☐ A Days to weeks — records must be reconstructed from emails and spreadsheets
- ☐ B Hours — records archived but not easily searchable
- ☐ C Minutes — stored but requires navigation
- ☐ D Seconds — single lookup; every action is timestamped and exportable

05.

**Workforce
Leverage**

As your credentialed network has grown over 3 years, what has happened to your credentialing headcount?

- ☐ A Grown proportionally — every 1,000 providers required additional FTEs
- ☐ B Grown faster — backlog pressure required headcount ahead of volume
- ☐ C Grown slower — some automation gains reduced the ratio
- ☐ D Stayed flat or declined — technology absorbed volume growth

Mostly A or B:

Significant infrastructure gaps. Regulatory changes in Section 3 represent near-term compliance risk. Start with Part I.

Mostly C:

Working foundation with identifiable gaps. Focus on Part II and Section 8 for next investment decisions.

Mostly D:

Mature operations. Use Part III and IV to validate your decision framework and sharpen your business case.



Who This Is Written For

This paper is written for two types of payer operations leaders who rarely read the same documents but are increasingly accountable to the same organizational outcomes.

The Operational Transformer

A VP managing credentialing operations, BPO vendor relationships, and workforce efficiency. Measured on turnaround times, staff productivity, and vendor quality. Overseeing in-house and outsourced credentialing, often with visibility gaps between what the BPO reports and what is actually happening in the network.

Reads this paper for:

- Hidden cost calculation framework (Section 1)
- Manual workflow diagnosis and barriers (Section 2)
- BPO vs. in-house decision matrix (Section 6)
- PSV automation benchmarks (Section 8)
- KPI definitions and pilot structure (Sections 7 & 9)

The Enterprise Governance Leader

A VP accountable for provider data integrity, audit readiness, and regulatory compliance across multiple lines of business — Medicaid, Medicare, Commercial. Managing provider portals, EDI, and credentialing as a federated function. Shifting operations from reactive execution to disciplined, risk-measured performance.

Reads this paper for:

- Fraud and claims risk framework (Section 1)
- Provider data governance model (Section 4)
- Ghost network measurement (Section 5)
- Regulatory compliance briefing (Section 3)
- Non-clinical AI pilot entry point (Sections 8 & 9)

→ Both leaders work in organizations where credentialing has historically been treated as a cost center. This paper argues that is the wrong frame — and offers both a different way to see it.



PART 1

Understanding the Problem

Section 1

What Credentialing Actually Costs

Most payer organizations know credentialing is slow. Fewer have measured what that slowness costs across the organization. The framework below surfaces all five dimensions — including two that most organizations have never formally calculated.

#	Cost Dimension	Typically Measured?	How to Calculate
01	Network Access Delay	Rarely	$\text{Avg. encounters/provider/month} \times \text{avg. days in queue} \times \text{avg. per-encounter margin}$
02	Staffing & Overhead	Rarely	$\text{Staff hours} \times \text{burdened rate} \div \text{credentials processed monthly}$
03	Vendor & Outsourcing	Partially	$\text{Per-file fee} \times \text{annual re-credential volume} + \text{overtages} + \text{coordination overhead}$
04	Fraud & Claims Risk	Almost never	$\text{Risk-adjusted exposure per provider} \times \text{monitoring gap in days}$
05	Regulatory & Audit Exposure	Almost never	$\text{Risk-adjusted audit liability} + \text{MA quality bonus exposure at current member scale}$



-
- 01 Network Access Delay Cost**
- When a provider spends 60–120 days in the credentialing queue, they are not seeing members. For high-demand specialties or underserved markets, that delay directly impacts network adequacy, member access, and competitive positioning.
-
- 02 Staffing and Overhead Cost**
- Credentialing built on manual verification requires staff proportional to volume. Most organizations have never formally measured cost per credential. When they do, the number surprises leadership.
-
- 03 Vendor and Outsourcing Cost**
- The CVO per-file fee model creates a direct link between network growth and cost with no volume efficiency. As networks expand into BH or new geographies, cost compounds. Most CVO contracts include annual rate escalators.
-
- 04 Fraud and Claims Risk**
- Providers who pass initial credentialing can still introduce financial and regulatory risk if credentialing is a one-time qualification checkpoint rather than a continuous monitoring function. Claims paid to sanctioned providers during a monitoring gap represent measurable, recoverable losses.
-
- 05 Regulatory and Audit Exposure**
- Inadequate credentialing infrastructure increasingly produces audit findings, CMS scrutiny, and — for MA plans — Star Rating impacts. Each CAHPS access-to-care Star Rating point represents \$200–500/member/year in quality bonus revenue at scale.
-
-
-
-
-
-
-
-



Section 2

Why the Process Has Stayed Manual

Credentialing has resisted improvement not because of lack of effort, but because the structural barriers are real and specific. Five barriers explain why the same inefficiencies persist across organizations of every size.

01 The Data Rebuilding Problem

Every payer independently rebuilds the same provider dataset from the same primary sources. CAQH is the closest the industry has come to a shared infrastructure, but it is not designed to maintain real-time accuracy. The redundancy is a consequence of fragmented regulation and the absence of a shared standard for what "credentialed" means.

02 The Verification Authenticity Barrier

Primary source verification is not uniformly accessible. State licensing boards, DEA, and board certification bodies increasingly deploy CAPTCHA protection, bot detection, and multi-factor authentication. Most automation solutions automate open sources and manually verify the rest — producing a process that looks automated but isn't. The diagnostic question: of your verification volume, what percentage requires a human to bypass a security barrier? That percentage is your true automation gap.

03 The Snapshot Problem

Re-credentialing every two to three years creates multi-year windows where a provider's status is assumed rather than verified. Licenses lapse. Sanctions are filed. Exclusions are added.

04 The Institutional Knowledge Trap

Manual credentialing workflows accumulate Institutional knowledge in coordinators. When a coordinator leaves, or when a BPO vendor transitions, that knowledge leaves too. Organizations running credentialing through outsourced relationships often discover they have less visibility into their own process than they believed. Vendor transitions expose this gap in the most disruptive possible context.



05 The Administrative Framing Trap

When credentialing is categorized as paperwork rather than a function affecting network safety, staffing models, access, and regulatory exposure, it does not receive the investment, measurement rigor, or leadership attention that would reveal its true cost. The framing creates and sustains the problem.

- The verification authenticity barrier deserves particular attention. Half of all primary source data sits behind bot detection, CAPTCHAs, and authentication barriers — including DEA. Vendors who claim full automation but fall back to manual verification for protected sources are solving a different problem. For evaluation purposes, this distinction is architectural — not a feature difference.



Section 3

The Regulatory Acceleration — Why "Wait and See" Has a Cost

The credentialing status quo was manageable when regulatory requirements were stable. They are not stable. The quick-reference table below summarizes what has changed and what each development requires of your current infrastructure.

Regulation /Standard	What Changed	Infrastructure Required	Urgency
NCQA 2025 HP Accreditation	PSV windows shortened 180→120 days; monthly SAM/Medicaid monitoring now required; explicit audit trail maintenance	Ongoing monitoring capability; audit records as ongoing system output, not reconstructable artifact	High — affects next accreditation cycle
MHPAEA Final Rule (2024)	BH NQTL requirements extend to network adequacy in practice; enforcement moving from guidance to active review	Continuous BH provider monitoring; adequacy analytics by specialty, not just point-in-time counts	High — enforcement active 2025–26
CMS Directory Accuracy	Movement toward public disclosure of error rates; directory inaccuracy now a market positioning issue	Real-time status propagation from credentialing to directory; monitoring lag measured and reported	Medium-High — disclosure risk rising
No Surprises Act	Inaccurate out-of-network listings create direct claims exposure and dispute liability	Status changes propagate to out-of-network listings within days, not months	Medium — claims exposure ongoing
MA Star Ratings	CAHPS access-to-care scores feed directly into Star Ratings and quality bonus revenue (\$200–500/member/year per point)	Directory accuracy at scale; provider accessibility data continuously maintained	High — revenue at risk, quantifiable



Diagnostic Questions — Ask Your Team

NCQA 2025

→ Diagnostic

Does your current process produce continuous audit records or reconstructed ones? Can you demonstrate monthly SAM/Medicaid monitoring to an auditor today?

Verifiable's credentialing platform is built against current NCQA HP accreditation standards, including shortened PSV windows and monthly monitoring requirements — noted here as a benchmark for what compliant infrastructure looks like, not as a recommendation.

MHPAEA

→ Diagnostic

What is your monitoring cadence for BH providers specifically? If a BH provider's license lapsed today, how quickly would your directory reflect that?

CMS Directory Accuracy

→ Diagnostic

How do you measure your directory accuracy rate? What is your process for catching status changes between re-credentialing cycles?

No Surprises Act

→ Diagnostic

What is your current lag between a provider leaving the network and that change propagating to your out-of-network listings?

MA Star Ratings

→ Diagnostic

If your directory accuracy rate is off by 5%, what is the estimated CAHPS access-to-care impact — and how does that translate to Star Rating revenue exposure at your current membership?



PART 2

Measure Your Baseline

Section 4

Measuring Your Current State: A Credentialing Maturity Framework

Before making decisions about technology, vendors, or operational models, payer operations leaders need a shared vocabulary for where they are. Use this as a team exercise before any evaluation begins. The maturity assessment tells you what you are solving for, which determines what you should be evaluating.

Dimension	Basic	Developing	Advanced
Verification Completeness	Manual outreach for majority of sources; no automation infrastructure	40–70% automated; protected sources still require manual workarounds	90%+ automated direct-to-source, including CAPTCHA-protected sources
Monitoring Frequency	Re-credentialing cycles (2–3 years) as primary monitoring mechanism	Monthly batch scans; license monitoring on 30-day cycles	Continuous surveillance; same-day alerts for adverse actions across all sources
Data Governance Integrity	Credentialing, directory, and claims maintain independent records; manual reconciliation	Credentialing is primary; directory sync has lag; some manual reconciliation	Single source of truth; status changes propagate automatically to all downstream systems



Dimension	Basic	Developing	Advanced
Process Auditability	Verification history reconstructed from emails, spreadsheets, and memory	Records archived; searchable with effort; some chain-of-custody gaps	Every action timestamped and exportable; full history is a single lookup
Workforce Leverage	Headcount scales linearly; every 1,000 providers requires additional FTEs	Some automation reduces ratio; headcount grows slower than network	Technology absorbs volume growth; FTE shifts to exception management and higher-value work

Use this as a team exercise before any vendor evaluation. Mismatches between what an organization thinks it needs and what it actually has are the most common source of failed technology investments in credentialing operations.

Section 5

The Ghost Network Problem — Measuring What You Don't Know

What the research shows: A 2023 review of physician directories from five large health insurers found that 81% of entries had inconsistencies such as address errors or the wrong specialty listed. That same year, a secret shopper study by the New York Attorney General's office called approximately 400 mental health providers listed as in-network in a state health plan and determined that 86% were ghost entries. The U.S. Senate Finance Committee's 2023 review of Medicare Advantage directories found that 33% of listed mental health providers had wrong numbers, were unreachable, or did not return calls.

Sources: 2023 multi-payer directory review; New York Attorney General's Office, 2023–24; U.S. Senate Finance Committee Majority Staff Report, May 2023.



Ghost networks are invisible until a member tries to use them. The gap between directory listings and actual network capacity surfaces as member complaints, access failure grievances, and adequacy audit findings — all downstream consequences of a problem that is detectable upstream.

A Framework for Measuring Directory Integrity

-
- | | | |
|-----------|--------------------------------|---|
| 01 | Outreach-Based Sampling | Select a random sample of listed providers across specialties and geographies. Attempt contact through listed information. Document the percentage reachable, in-network, and accepting new patients. Low-tech but produces a real accuracy rate. |
|-----------|--------------------------------|---|
-
- | | | |
|-----------|-------------------------------|---|
| 02 | Claims Cross-Reference | Compare directory listings against recent claims activity. Providers listed as active with no claims activity over a meaningful window are candidates for verification. Works at scale but requires data access across systems. |
|-----------|-------------------------------|---|
-
- | | | |
|-----------|--------------------------------------|--|
| 03 | Re-Credentialing Gap Analysis | For each network provider, calculate time elapsed since last primary source verification. Segment by elapsed time. Providers furthest from their last verification are the highest-risk directory entries. |
|-----------|--------------------------------------|--|
-
- | | | |
|-----------|--|---|
| 04 | Monitoring Frequency and Coverage | What is your current cadence for sanctions and exclusion checks? How much regulatory exposure does your organization carry if cadence or source coverage is insufficient? Run this analysis by line of business and geography |
|-----------|--|---|
-
- | | | |
|-----------|--------------------------|--|
| 05 | Adequacy Modeling | For each specialty and geography, compare listed providers against providers who are actually reachable and accepting patients. The gap is your adequacy overstatement — the number that matters to CMS, NCQA, and state regulators. |
|-----------|--------------------------|--|
-



→ Behavioral Health — A Distinct Risk Category

BH provider attrition is meaningfully higher than medical/surgical. Any directory integrity measurement should treat BH networks as a distinct segment with its own accuracy assessment. The MHPAEA enforcement trajectory means BH adequacy overstatements are no longer just a member experience problem — they are a regulatory exposure. The New York AG action against EmblemHealth in early 2026 — a \$2.5M penalty and member reimbursement requirement tied directly to BH ghost network rates — illustrates where enforcement is heading.

Organizations managing BH networks at scale find that continuous license monitoring, not periodic re-credentialing, is the only operationally defensible model. Grow Therapy, which onboards over 1,000 new providers monthly across all 50 states, uses automated monitoring as the foundation of a model where new patients can be matched with therapists within 3–4 days of their request.



PART 3

Making the Decision

Section 6

Choosing an Operational Model: A Decision Framework

There is no single right answer to how payer credentialing should be structured. The right model depends on network size, growth trajectory, existing infrastructure, workforce capabilities, and regulatory context. This section provides a framework for making that decision, not a recommendation.

→ The Three Primary Models

Dimension	How It Works	Best For	Key Tradeoffs
In-House with Technology	Credentialing team uses software to automate PSV, manage workflows, and maintain monitoring. Full process visibility and control retained internally.	Plans with active credentialing teams, growth mandates, and desire for process control.	Requires internal capability building. Higher upfront investment. Returns proportional to network size.
Outsourced CVO	External organization manages the full process. Plan pays per file or per provider credentialed.	Plans without internal infrastructure; overflow management; mid-technology transition.	Per-file cost scales with volume — no efficiency gain. Limited visibility. Vendor dependency.
Hybrid	Software handles core volume; CVO handles overflow, complex cases, or specific lines of business.	Large plans with mixed needs; enterprise organizations managing multiple LOBs.	Requires clear scope definition. Works well when the split is intentional and measured.



ROI Decision Matrix

The economics of each model shift depending on two variables: network growth urgency and your current operational model.

Dimension	In-House / Manual Today	Outsourced CVO Today
High Growth Urgency	Software + AI Automation Prime candidate for automation. Manual processes will not keep pace with growth. Cost per credential drops as volume increases.	Insource + Automate CVO per-file fees scaling with your network. Transition to in-house software converts variable cost to fixed. Hybrid model is a valid bridge.
Low Growth Urgency	Targeted Automation Focus automation on monitoring and auditability rather than volume throughput. Regulatory improvements deliver ROI regardless of growth rate.	Cost + Quality Assessment Benchmark current CVO cost per credential against in-house alternatives. Ensure your CVO contract includes audit rights and quality SLAs.

→ For BPO and consortium contexts:

The framework above applies when credentialing is managed by a BPO — but you are also evaluating the vendor's operational model. Define quality metrics contractually. Multi-entity credentialing consortiums face a compounding version: inefficiency in shared infrastructure is magnified across all participating entities.



Section 7

Building the Internal Business Case

For most payer operations leaders, investing in credentialing transformation requires making a case to a CFO, CIO, or COO who may not have detailed familiarity with what credentialing does. The translation work is yours.

Translating Credentialing into Executive Language

CFO Frame

→ Variable Cost to Fixed

Software + AI Automation

Days of delayed claims activity per provider

Manual verification

Cost per credential and headcount required at scale

Directory inaccuracy

Adequacy audit exposure + Star Rating revenue at risk (MA plans)

Re-cred cycle gaps

Risk-adjusted exposure on every dollar paid during monitoring gap

CIO Frame

→ Infrastructure Risk

Data fragmentation

Data debt compounding over time across credentialing, directory, claims, enrollment

Manual output

Non-standardized records that cannot be audited, reported on, or integrated downstream

Credentialing infra

Prerequisite for provider data quality supporting VBC programs, analytics, and risk management

COO Frame

→ Operational Scalability

Headcount-to-network

Is this relationship linear? At what network size does it become untenable?

BPO management load

How much team time is spent monitoring a vendor vs. improving the process?

Network-to-market time

Days between a provider signing a contract and seeing their first member



The Six KPIs That Matter

Define these metrics before any pilot begins. Results are only attributable if the baseline is established in advance.

KPI	What It Measures	Executive Translation
Days to Credential	Application received → approval. Primary throughput metric.	Network access delay and competitive speed to market
Cost per Credential	Total credentialing spend ÷ credentials processed monthly.	Most organizations have never calculated this. It is the CFO's number.
Error / Flag Rate per File	Verifications requiring manual correction or escalation.	Tracks quality, not just speed. Liability indicator for governance.
Directory Accuracy Rate	% of listed providers reachable, in-network, and accepting patients.	Star Rating input for MA plans. CMS disclosure exposure for all plans.
Monitoring Lag	Max days between provider status change and system detection.	Compliance posture metric. The number regulators ask about.
Audit Readiness	Time to produce a full verification history for any provider on demand.	Seconds = advanced; days = basic. Determines audit outcome before the auditor arrives.



Section 8

What to Look For When Evaluating Credentialing Technology

If the decision framework in Section 6 points toward technology investment, the criteria below apply regardless of which vendors are in consideration. The questions are designed to produce genuinely differentiated answers, not vendor marketing language.

The Verification Authenticity Question: Ask Every Vendor

Primary sources are not uniformly accessible. State licensing boards, DEA, and board certification bodies increasingly deploy CAPTCHA protection, bot detection, and multi-factor authentication barriers. **The right question to ask any credentialing technology vendor:**

“ For each source you claim to verify, is that verification automated directly to the primary source, or does it involve a human workaround at any point?

The answer matters because solutions that fall back to manual verification for protected sources produce inconsistent output and still carry human error risk. True primary source automation that includes CAPTCHA-protected and authenticated sources is architecturally different and produces materially more reliable verification at scale.

Evaluating Credentialing Software

Source coverage: How many primary sources, for which provider types and states?

Automation rate: % of verifications returning without human intervention. (Benchmark: documented pilots show 6–8× reduction in data review time per 10 providers, via parallel processing rather than linear time savings.)

Monitoring frequency: Typical lag between a source change and a system alert?

Auditability: Every action traced, timestamped, and exportable?

Configurability: Workflows configurable to your specific NCQA policies?

Evaluating CVO Services

TAT SLAs: What is contracted vs. actual turnaround time performance?

Error rate: How is quality measured? What does the contract say about remediation?

Source transparency: Can you audit their verification records for any provider?

Transition risk: What is the cost and complexity of moving in-house or switching vendors?

Multi-entity fit: Does the vendor model support BPO/consortium arrangements?



Evaluating AI in Credentialing

AI in credentialing is genuinely useful in two distinct contexts: (1) automating high-volume, rule-based verification tasks, and (2) reviewing completed packets for flags that human review may miss at scale. These are different capabilities. Ask vendors to be specific about which they are offering — and what the audit trail looks like for each.

Question to Ask	What a Strong Answer Looks Like	What to Watch Out For
Is the AI end-to-end or task-specific?	Orchestrates the full credentialing workflow — intake, PSV, packet generation, review — with human checkpoints	Claims "AI-powered" but applies automation only to a single step (e.g., OCR on uploaded documents)
What happens at protected sources?	Direct API connections to CAPTCHA-protected and authenticated sources; no human fallback	Falls back to manual verification for DEA, state boards, or other protected sources
What is the audit trail?	Step-by-step decision logs with cited primary sources for every verification action	Black-box output with no traceable decision path — undiscoverable in an audit
How is accuracy validated?	Offline testing against real-world scenarios before deployment; live trace monitoring; defined confidence thresholds	Accuracy claims without documented test methodology or error rate measurement
How does it handle state-specific nuances?	Configurable rules for state-by-state disclosure questions, license requirements, insurance minimums	One-size-fits-all processing that doesn't account for multi-state provider complexity

→ **Point of reference:** Verifiable's CredAgent™ condenses 150 credentialing steps into 3 human review checkpoints — data review, verification checkpoint, and packet checkpoint. It is cited here as one example of end-to-end agentic design. The evaluation table above applies to CredAgent and every other vendor making AI credentialing claims equally.

For AI governance committees: credentialing is non-clinical, fully auditable, and carries no patient-facing decision-making risk — making it one of the lower-risk, higher-ROI entry points for AI deployment in payer operations.



PART 4

Implementation

Section 9

Structuring a 90-Day Pilot

Credentialing is well-suited to a time-bounded AI pilot because the inputs, outputs, and success criteria are clearly defined, the domain is non-clinical, and results are attributable within a short window.

→ Pilot Design Principles

01.

Define scope narrowly — a specific provider group, specialty, geography, or line of business

02.

Establish baseline metrics before the pilot begins — you cannot demonstrate improvement without a "before"

03.

Run the pilot in parallel with your existing process initially to validate accuracy before full transition

04.

Define success criteria in advance and in writing — what numbers constitute a successful result?

05.

Maintain non-clinical framing throughout — no patient-facing systems, no clinical decision-making



Phase	Timeline	Deliverable	Owner
Baseline Measurement	Weeks 1–2	Current TAT, cost per credential, error rate, and staff hours documented against the 7 KPI definitions from Section 7	Operations lead
Cost per Credential	Weeks 2–4	Provider group selected, pre-credentialing criteria defined, process design documented and approved	Operations + Technology
Parallel Run	Weeks 4–8	New process runs alongside existing; accuracy comparison tracked; discrepancies logged and addressed	Operations lead
Full Transition	Weeks 8–12	New process runs independently; all KPIs tracked against baseline; anomalies escalated immediately	Operations + Technology
Results Documentation	Week 12	Before/after comparison across all KPIs; ROI calculation; recommendation for full rollout or adjustment	Ops lead + Exec sponsor

→ Risk Profile Statement

Non-Clinical

No patient-facing decisions.
No clinical data. No care pathway impact.

Low-Risk

Process automation on administrative data.
Regulatory exposure is reduced by improved monitoring, not increased.

High-ROI

Seven-figure savings documented. Measurable in 90 days. Staff hours, cycle time, and error rate all quantifiable.

This framing is specifically designed for AI governance committees and risk-averse technology leaders. Credentialing pilots require no patient-safety governance, no FDA consideration, and no clinical validation pathway. They do require operational discipline and defined KPIs — both of which are in scope for the payer operations leaders reading this paper.

For multi-LOB enterprises: Run the pilot on a single line of business first. The governance frameworks, measurement systems, and operational learnings transfer to other lines of business before expanding scope.



Conclusion

The Limiting Factor Is Priority, Not Technology

Credentialing has the tools available to operate as a genuine strategic capability. The infrastructure exists. The ROI is measurable. The regulatory urgency is real and accelerating.

The organizations that treat this as a strategic moment — rather than a compliance maintenance task — will have meaningfully better networks, lower risk exposure, and more scalable operations than those that don't. They will also have the provider data infrastructure that makes every other strategic capability — value-based care programs, network adequacy analytics, AI in operations — actually work.

The most common limiting factor is not technology. It is organizational prioritization: treating credentialing as back-office overhead rather than a function with measurable impact on network accuracy, access, and financial performance. Changing that frame is the first move.

→ The frameworks, diagnostic questions, and decision tools in this paper work with any vendor, any operational model, and any technology stack. The goal is not a specific answer — it is a better way of asking the question.

A note on co-authorship:

Verifiable, as co-publisher of this paper, has built its credentialing platform around this premise — that the infrastructure for treating credentialing as a strategic function already exists. That context is disclosed, not hidden. Joey Costa of Provider Peak serves as primary author and independent practitioner voice. The frameworks in these pages were written to be useful whether or not Verifiable is part of the answer.



Reference Case Studies

Organization	Context	Source
Humana Dental	98% TAT reduction, 7-figure savings, 50% admin overhead reduction, 25% network growth on insource	verifiable.com/resources/case-studies/humana-dental-case-study
Access TeleCare	67% TAT reduction; 250+ page packets generated automatically; 18mo deployment cycle eliminated	verifiable.com/resources/case-studies/access-telecare-on-verifiable
Midi Health	1–2 day NP credentialing TAT; full credentialing across 50 states via automated data collection	verifiable.com/resources/case-studies/midi-health-on-verifiable
Modern Health	BH network credentialing at scale; provider NPS on onboarding increased; single source of truth achieved	verifiable.com/resources/case-studies/modern-health
Grow Therapy	1,000+ providers onboarded monthly; new patients matched in 3–4 days; NCQA certification as payer selling point	verifiable.com/resources/case-studies/grow-therapy
ROI Calculator	Estimate cost per credential and payback period for in-house transition	verifiable.com/resources/roi-calculator





I've seen health plans where it takes six to eight months to credential a provider and that's not acceptable. At Humana, we wanted to come up with the most efficient, streamlined way to credential. When we started to really utilize Salesforce to the fullest, thanks to Verifiable, we began seeing real benefits.

Dara McDaniel

Associate Director of Credentialing and Compliance

Humana



No other platform had the customization or the flexibility that we saw with Verifiable. This flexibility allowed us to reduce turnaround times by 67% — onboarding providers 3× faster — which is priceless for ensuring our clients get the acute specialty care coverage they need.

Lara Galaviz

VP of Provider Network Operations

 **Access**
TeleCare



Our consistent turnaround times combined with a robust focus on NCQA standards has become a top selling point when facilitating contracts with new payor partners. Before, our provider intake form used to take providers 20–30 minutes. Now, we can cut the completion time down to 10 minutes.

Christy Maselli

Credentialing Lead

growththerapy



Independent References

Source	Finding
2023 multi-payer physician directory review	81% of entries contained inconsistencies — address errors, wrong specialty, unreachable providers
New York Attorney General's Office, 2023–2024	~400 BH providers called in one state health plan: 86% were ghost entries. EmblemHealth agreed to \$2.5M penalty.
U.S. Senate Finance Committee Majority Staff, May 2023	Secret shopper study: 33% of 120 MA mental health directory listings were wrong numbers, non-working, or unreturned
AHIP Statement to Senate Finance, May 2023	Acknowledged directory accuracy as a "longstanding issue"; confirmed provider self-reporting delays as a structural driver
PwC Health Research Institute (2025 projection)	8% YoY medical cost trend for Group market — operational efficiency in network management is a direct cost containment lever
AHIP 2024 Annual Meeting	AI and data standardization identified as top health plan investment priorities — credentialing operations a natural first deployment target





ABOUT THE AUTHOR

Joey Costa

joey@providerpeak.com

+1 412 973 5652

providerpeak.com

Joey Costa is the Principal of Provider Peak, a healthcare advisory firm focused on improving financial performance and access across the healthcare ecosystem. He advises senior executives, independent physician groups, payers, TPAs, and healthcare enablers on how to design, negotiate, and operate high-performing provider networks in today's highly consolidated healthcare landscape.

His work centers on helping organizations reorient contracting, pricing transparency, and network strategy to meet the realities of rising costs, shifting site-of-care dynamics, and the growing urgency to strengthen independent specialty care.

Previously, Joey served as Executive Vice President of Provider Network at Lantern (formerly Employer Direct Healthcare), a member of the Executive Management Team responsible for the nation's largest direct-to-employer surgical benefit. He oversaw an eight-figure P&L, led provider network operations serving 4M+ members, and drove enterprise-wide growth initiatives including transformational revenue expansion, next-generation network design, national cancer-care partnerships, and quality programs.

Before that, Joey led national managed-care strategy at Care Centrix (19M covered lives); held leadership roles at Oscar Health, where he executed the company's shift from leased networks to a directly contracted model and helped scale revenue past \$1 billion; and began his career at PwC supporting Fortune 50 organizations on vendor strategy, regulatory remediation, and operating-model redesign.

Joey holds an Executive MBA in Healthcare from the University of Pittsburgh (Outstanding Student of the Program), a Master of Public Health in Management from Columbia University, and a BS in International Relations and International Business from Syracuse University. He resides in Pittsburgh, Pennsylvania.



Provider Peak is a healthcare advisory firm focused on improving financial performance and access across the healthcare ecosystem.

Services

- Payer contracting & reimbursement strategy
- Provider network optimization for payers & TPAs
- Pricing transparency & data analytics
- Revenue growth strategy
- Healthcare technology advisory

Provider Peak maintains transparent partnerships with select healthcare technology and enablement companies.





Healthcare Credentialing & Provider Network Platform

Verifiable is a healthcare credentialing and provider network management platform built to help payer and provider organizations speed up network operations, reduce costs, and maintain continuous regulatory compliance. The company's mission is to rebuild the infrastructure of trust in healthcare by transitioning the industry from manual credentialing workflows to a new standard powered by agentic AI.

Founded in 2019 by Nick Macario and Vivekanand Rajkumar and headquartered in Austin, Texas, Verifiable was built API-first to connect directly to primary sources — state licensing boards, DEA, CAQH, OIG, NPDB, and 3,200+ additional verification types — delivering real-time results rather than batch processing. The platform is a native Salesforce application and integrates with existing CRM infrastructure without requiring a wholesale system change.

In February 2026, Verifiable launched CredAgent™ — the industry's first autonomous AI agent for end-to-end credentialing. CredAgent condenses 150 credentialing steps into 3 human review checkpoints, processes thousands of providers in parallel, and provides step-by-step decision logs with cited primary sources for every verification action. Unlike tools that automate isolated tasks, CredAgent orchestrates the full workflow while maintaining full auditability and configurability against each organization's NCQA policies and business rules.

Verifiable offers three delivery models: in-house software, an NCQA-certified CVO with a <3 day turnaround time and 100% audit pass rate, and a hybrid model. The company has raised \$50.1M in total funding from Y Combinator, Tiger Global, The Altman Fund, Craft Ventures, Highland Capital Partners, and Struck Capital, among others.

→ Platform at a Glance

Founded

2019, Austin, Texas

Primary sources

3,200+ verification types

Automation rate

97% of PSVs returned automatically

Delivery models

Software · CVO · Hybrid ·
Monitoring-only

Salesforce

Native application; 100+
Salesforce customers

CVO

NCQA-certified; <3 day TAT;
100% audit pass rate

CredAgent™ NEW

Up to 10× productivity; 150 steps
→ 3 human review points

Investors

Y Combinator, Tiger Global,
The Altman Fund, Craft Ventures



Next Step

Schedule Your Credentialing Maturity Workshop

A working session, not a sales call, designed to produce two things: a clear picture of where your credentialing operations stand today, and a business case you can present internally.

01. Maturity Assessment

- Score your organization across all five dimensions from Section 4
- Identify your highest-priority gaps — by line of business if needed
- Benchmark against what peer payer organizations have measured

02. Cost and Risk Quantification

- Calculate your actual cost per credential using the framework from Section 1
- Quantify monitoring lag and audit exposure
- For MA plans: estimate Star Rating revenue at risk from directory inaccuracy

03. Business Case Development

- Frame findings in CFO, CIO, and COO language (Section 7)
- Define the right operational model for your organization — in-house, outsourced, or hybrid
- Leave with a 90-day pilot structure ready to present

Non-Clinical

The workshop is designed for VP-level payer operations leaders who have read this paper and want to apply the frameworks to their own organization. It works best when two or three internal stakeholders attend — typically an operations lead, a technology or data lead, and an executive sponsor.

Format & Logistics

Duration: 30 minutes (virtual or in-person)

Participants: 2–4 from your organization + Joey Costa

Pre-work: NCQA-certified; <3 day TAT; 100% audit pass rate

Output: Maturity scorecard, cost quantification, and draft business case

Cost: No charge for qualified payer organizations



Schedule Your Credentialing Maturity Workshop

Schedule your workshop at providerpeak.com or reach Joey directly
joey@providerpeak.com | 412.973.5652

Co-published with  **Verifiable**