

One ACO, many systems

Building a trusted identity foundation for value-based care

How Medicare Shared Savings Program, ACO REACH and commercial ACOs create a reliable view of their attributed population across independent providers, EHRs, and care settings.

Inside this paper

- Why a stand-alone ACO cannot reliably see its own attributed population
- Where fragmented identity quietly degrades cost, quality, and physician trust
- Why EHRs and population health platforms cannot carry identity on their own
- What patient and provider identity look like as shared network infrastructure
- A 12-statement identity-readiness self-assessment you can score today

Prepared for: chief medical officers, population health leaders, and value-based care professionals.

Published: August 2026

Executive Summary

Stand-alone accountable care organizations (ACOs) are asked to do something structurally and operationally difficult: They accept accountability for the total cost and quality of a defined population that receives care across organizations the ACO does not own, documented in electronic health records the ACO does not control, in settings the ACO often cannot see into. Substantial investment has gone into closing that gap through analytics and platform strategy. The constraint that remains sits one layer below both of these solutions. **That constraint is identity.**

Most ACOs cannot answer a deceptively simple question with confidence: who is actually in this population, and is this person the same person already known from somewhere else in the network? When one patient exists as four records across four independently owned practices, the ACO does not have one patient. It has four partial patients. Every downstream function inherits that fragmentation, from care gap closure and outreach to the longitudinal record at the point of care, quality reporting, cost and utilization analytics, and the basic question of which participant owns the relationship.

Patient and provider identity is not an analytics feature to be purchased inside another tool. For a stand-alone ACO, it is shared network infrastructure, determining whether investments from population health and health information exchange to care management perform as intended. The scale and success of the Shared Savings Program rest on an assumption that is rarely examined: that an ACO can reliably and continuously identify its patients and where they are receiving care.¹

480

Shared Savings
Program ACOs
(as of January
2024)

608,000

clinicians providing
care to nearly 11
million people with
Medicare

**\$2.1
billion**

in net savings
in 2023

**\$3.1
billion**

in shared savings
payments earned by ACOs

The evidence says that assumption often fails. Facilities fail to link records for the same patient as often as half the time, with match rates as low as 50% even between organizations sharing the same EHR vendor.³ A national analysis of Medicare ACOs found that each percentage point increase in out-of-network primary care was associated with a \$10.79 increase in quarterly per beneficiary spending, and its authors observed that ACOs have few sight lines into and even less control over care delivered outside their boundaries.⁴

THE HEADLINE FOR ACO LEADERS:

A patient who cannot be resolved across participants is not a data quality inconvenience. That patient is invisible to stratification, absent from the quality numerator, missing from the panel report and unavailable to the care manager, while remaining fully present in the total cost of care the ACO is accountable for.

1. Where fragmented identity damages performance

Fragmented identity rarely announces itself as an identity problem. It shows up as a care gap that was already closed, an outreach call to a patient who moved two years ago, a measure denominator nobody trusts, or a physician who says the panel report does not describe the patients they actually see. Each of those is a downstream symptom of one upstream failure: the inability to say with confidence that two records describe the same person, or that a clinician genuinely practices where the directory claims.



Care gaps and outreach

Care gap logic assumes a complete record. When a diabetic eye exam performed at an unaffiliated ophthalmology practice cannot be linked to that patient's record in the population health platform, the gap stays open, the outreach team calls anyway, and the patient is asked to repeat a service they already received. The cost lands in three places at once: staff time spent on unnecessary work, physician and patient confidence in the program, and in some cases a duplicated service the ACO ultimately pays for.

Outreach fails for a second and quieter reason: the contact information is stale. A phone number disconnected two years ago and an address three moves old are not identity errors in the strict sense, but they defeat the campaign just as completely. Identity resolution establishes who the person is; Verato Enrich® can then append verified outreach data such as phone, email, and address.



The longitudinal record at the point of care

The inverse error is the more damaging one, and it is far harder to see. A patient whose history is split across two identities appears in the data as two lower-acuity patients rather than one high-risk patient and never rises to the top of a stratification list. Care management capacity is finite, and it is allocated from exactly that data. Identity errors therefore do not simply add noise to the analytics; they point the most expensive resource an ACO has at the wrong people. What remains at the point of care is a record that looks complete to the clinician reading it while being materially incomplete in ways no one in the room can detect. Nobody files a ticket when a patient fails to appear on a list.



“ Nobody files a ticket when a patient fails to appear on a list.



Quality reporting, risk adjustment, and analytics

Measurement inherits every identity error beneath it, and the errors run in both directions.

- Numerators are missed when the qualifying service happened elsewhere under an unmatched identity, and denominators are inflated when one person is counted twice. Under all-payer electronic clinical quality measure reporting, where the ACO reports across its entire population rather than a sample, matching reliability becomes a direct determinant of the reported score. An organization can deliver excellent care and report mediocre performance because its data cannot be assembled.
- Risk adjustment carries the same dependency in reverse. When data cannot be matched across independent participants, legitimate conditions documented elsewhere never reach the ACO's record, risk scores understate the population, and benchmarks are set against a panel that looks healthier than it is.
- Analytics inherit both problems. A cost and utilization report built on fragmented identity returns a confident-looking answer to a question no one asked, which is the most expensive kind of wrong.



Who owns the relationship

A final effect rarely appears in a business case. Identity determines whether physicians accept the ACO's analytics at all. Attribution reports and panel lists persuade only when a physician recognizes the names on them. A report containing patients they have never seen, or missing patients they manage closely, is dismissed in the first ten minutes of the meeting, and the performance conversation is dismissed along with it. Provider affiliation errors do more damage to physician trust than most disagreements about clinical targets, because they are so easy to verify and so hard to defend.

2. Why EHRs and population health platforms are not enough on their own

The capability is real, the scope is the problem

The argument here is not that electronic health records and population health platforms lack identity capability. They have it, and in many cases it is sophisticated. Every major EHR maintains a master patient index. Every serious population health platform performs some form of record matching as it ingests claims and clinical feeds. The limitation is not quality, it is scope. Each system resolves identity inside its own boundary, for its own purposes, using the data it happens to hold.





Every organizational boundary is a seam

For a stand-alone ACO, that boundary is exactly the problem. One participant's EHR resolves identity for that participant's patients. A second participant's instance does the same work independently. Neither is accountable for reconciling the two, nor was designed to be. The population health platform sits above both and inherits whatever quality the upstream feeds carry, which is why the platform so often takes the blame for a defect it did not create.

The cost of that design shows up on every change. When an ACO adds a participant, replaces a vendor or takes on a new payer contract, matching logic embedded inside each application has to be rebuilt or retuned, because it was never designed as a shared asset. Organizations end up paying for the same identity work repeatedly across a handful of years without ever owning the result.



What the national data shows

The national data suggests the connective tissue between systems is thinner than most executives assume. Even when clinical information from outside providers is available, it does not necessarily make its way into routine clinical use.⁵ The distance between available and used is a trust and usability gap, and the identity sits underneath both.

43%

of non-federal acute care hospitals routinely engaged in all four domains of interoperable exchange⁵

27%

did so sometimes⁵

71%

reported routine access to necessary clinical information from outside providers⁵

42%

said clinicians routinely use that information when treating patients⁵



More exchange is not the same as more clarity

The disconnection is worst in precisely the settings that drive ACO spending. Only 16% of hospitals reported sending summary of care records to most or all long-term and post-acute care providers, and 17% did so for behavioral health providers.⁵ National initiatives such as the Trusted Exchange Framework and Common Agreement are built to widen that pipe, and they matter. But a wider pipe delivers more records that still have to be matched to the right person and the right clinician. Exchange volume without an identity layer increases the reconciliation burden rather than resolving it.

3. Patient and provider identity as shared network infrastructure

Treating identity as infrastructure means building it once, governing it deliberately and distributing it to every system that needs it, the same way a health system treats authentication or a terminology service. It is additive rather than disruptive. Nothing here asks an ACO to replace an electronic health record or a population health platform. It asks for a layer underneath them that makes their outputs trustworthy.

Four components define that layer:



Patient resolution

Patient resolution is the ability to state, with a measured and auditable level of confidence, that records originating in different organizations describe the same person. For ACO leaders, the essential requirements are a network-level identifier independent of any participant's medical record number, consistent matching across every incoming feed, a stewardship process for uncertain cases, and routine measurement of match rates, duplicate rates, and manual review volume. Verato MDM Cloud™ applies Verato Referential Matching®, its patented approach to referential matching, to every participant feed and payer roster, which is why it resolves the records that defeat probabilistic matching.





Provider identity and affiliation

Provider identity is the half of the problem most organizations underinvest in, and the half that attracts the least executive attention. The clearest federal evidence remains the CMS online provider directory review, which examined 5,832 providers across 54 Medicare Advantage organizations and found 45.1% of the listed directory locations inaccurate, with the inaccuracies most likely to prevent access to care present in 38.4% of all locations.⁶ What matters more than the number is the diagnosis CMS attached to it. Group practices tend to supply data at the group level rather than the clinician level, so a physician is listed at every location the group operates even when that physician rarely or never practices there. CMS went on to call for a centralized repository for provider data accessible to multiple stakeholders. That is a description of shared identity infrastructure, written by the regulator.



Three capabilities make it real for an ACO:

- 1 One record per clinician, carrying the locations and panels where they actually practice, maintained as they move between participating organizations.
- 2 Attribution that keeps pace with physician movement rather than resetting on an annual cycle, so panel reports stay accurate between refreshes.
- 3 The ability to show which clinician, at which location, was accountable for a given attributed patient in a given period, and to prove it from the record.



Governance

Governance is what turns a matching engine into a trusted service. It defines who sets match thresholds and on what evidence, what happens when a merge is wrong and how it is unwound, which participants may contribute and consume identity data and under what agreements, how consent and minimum necessary requirements are honored across independently owned organizations, and how the arrangement is audited. None of that is abstract. The Government Accountability Office, in its congressionally mandated review of patient record matching, concluded that inaccurately matched records can adversely affect patient safety or privacy, and that no single effort would solve the challenge.²



Downstream distribution

An identity layer that nothing consumes changes nothing, and this is where well-funded programs most often fail quietly. Distribution means pushing resolved identity back out to the systems where the work actually happens: the population health platform, the care management workflow, the quality reporting pipeline, the analytics environment, outreach tools, and, where contracts permit, the participants' own electronic health records. It has to arrive through interfaces those systems consume natively, refresh on a defined cadence, and be instrumented so the organization can see which downstream systems are current and which have drifted.

4. Connecting identity to ACO economics

Three published findings anchor the economic case for connecting identity. Precision about what each one proves and what it does not is essential, because overstating the evidence is how sound arguments lose credibility in front of a finance committee.

FINDING	WHAT IT PROVES, AND WHAT IT DOES NOT
 Each percentage point increase in out-of-network primary care = a \$10.79 increase in quarterly per beneficiary spending in Medicare ACOs.⁴	An association drawn from national Medicare claims, not a causal estimate. It remains the clearest published link between care an ACO cannot see and the spending it is accountable for.
 ~18% of records are duplicates; repeated services attributable to duplicates cost roughly \$1,950 per patient per hospital stay, and about a third of denied claims stem from identification error.³	Hospital operating data summarized in 2018, not ACO shared savings data. Use it for the order of magnitude of duplication cost, not as a savings projection.
 45.1% of reviewed Medicare Advantage provider directory locations were inaccurate, and 38.4% carried the kind of inaccuracy most likely to prevent access to care.⁶	A 2016 CMS review of Medicare Advantage directories rather than ACO networks. The diagnosis travels further than the number: group-level data submitted in place of clinician-level data.

Read together, the pattern is consistent. Identity does not restrict where a patient goes, and it does not by itself close a single care gap. What it does is determine whether the ACO can see the encounter, recognize the patient, credit the right physician and act while the decision still matters.

IN PRACTICE

A major Texas health system using Verato to establish a Consumer 360 and enrich outreach data reported:

35%

improvement in care-gap campaign conversion

2%→26%

increase in email click rate



5. ACO identity-readiness assessment

The assessment below is designed to be completed jointly by operations, clinical, and analytics leadership, because the failure modes it describes cross all three functions and no single one of them can see the whole picture. Score each statement from 1 (not true today, no work underway) to 5 (true consistently, measured and governed). A 3 means partially true, or true for some participants and not others, which is where most networks actually sit. 12 statements, 60 points.

ONE RULE BEFORE YOU SCORE. Answer as your data would answer, not as your roadmap would. A capability that lives in a project plan has not yet resolved a single patient record.

DOMAIN	STATEMENT	SCORE 1-5
 Cross-system patient identity	We can state our current cross-participant match rate and duplicate rate from measurement rather than estimate.	
	A network-level patient identifier exists that is independent of any single participant's medical record number.	
	Every participant feed, payer file and external source passes through the same matching logic and the same stewardship process.	
 Data distribution	Resolved identity is delivered back to the population health platform, care management workflow and analytics environment on a defined cadence.	
	We can see which downstream systems hold current identity data and which have drifted.	
	Adding a participant, payer contract or vendor platform does not require rebuilding matching logic inside each application.	
 Provider identity and affiliation	We maintain a single source of truth for participating clinicians, their practice locations and their active affiliations.	
	Affiliation is verified at the individual clinician level rather than accepted at the group level.	
	Physicians receiving attribution and panel reports recognize the patients on them as their own.	
 Downstream workflow reliability	Care gaps closed outside the ACO are reflected in outreach lists before the patient is contacted.	
	Quality measure numerators and denominators can be traced back to resolved patient identities.	
	Identity decisions, including merges and unmerges, are governed, auditable and owned by a named accountable leader.	

YOUR TOTAL (add all 12 scores)	WHAT IT MEANS
	45–60: Identity is infrastructure Identity functions as a shared service rather than a feature of individual systems. The priority shifts from building the capability to sustaining it as participants, payers and platforms change.
	28–44: Partial foundation Usually strongest in patient matching and weakest in provider affiliation and downstream distribution. Invest in the weakest domain, because that is the one setting your performance ceiling.
	12–27: Exposure exists Identity is being handled incidentally by individual applications. Treat cross-system reporting and care management results as directional, and start with measurement: establish current match and duplicate rates before selecting any solution.

Whatever the total, the question underneath it is the one this paper opened with. If an ACO is accountable for a population distributed across organizations it does not own, recorded in systems it does not control, then the ability to recognize that population reliably is not an information technology project.

It is the precondition for everything else the organization is paid to do.



See exactly where your exposure lives

The 12-question assessment is a starting point. Verato works with ACOs to quantify duplicate-record rates, provider-attribution gaps, and chart-review linkage across every participating EHR and to build the identity layer that solves for each of these pain points.

TAKE THE NEXT STEP

Request your personalized readiness assessment

Get a confidential, organization-specific read on your identity exposure and get insights from industry leaders at Verato on a prioritized path to close it.

Visit verato.com to learn more.



Sources

- ¹ Centers for Medicare & Medicaid Services. Medicare Shared Savings Program continues to deliver meaningful savings and high-quality health care. News release. October 29, 2024. Accessed August 13, 2026.
- ² US Government Accountability Office. Health Information Technology: Approaches and Challenges to Electronically Matching Patients' Records Across Providers. GAO-19-197. January 15, 2019. Accessed August 13, 2026.
- ³ Genevieve Morris et al. (2014). Patient Identification and Matching Final Report [PDF]. Office of the National Coordinator for Health Information Technology.
- ⁴ Lin SC, Yan P, Moloci N, et al. Out-of-network primary care is associated with higher per beneficiary spending in Medicare ACOs. Health Affairs. 2020;39(2):310–318.
- ⁵ Gabriel MH, Richwine C, Strawley C, Barker W, Everson J. Interoperable Exchange of Patient Health Information Among US Hospitals: 2023. ONC Data Brief No. 71. Office of the National Coordinator for Health Information Technology; May 2024. Accessed August 13, 2026.
- ⁶ Centers for Medicare & Medicaid Services. Online Provider Directory Review Report. January 13, 2017. Accessed August 13, 2026.
- ⁷ Office of Inspector General, US Department of Health and Human Services. Medicare Advantage: Questionable Use of Health Risk Assessments Continues to Drive Up Payments to Plans by Billions. OEI-03-23-00380. October 2024. Accessed August 13, 2026.



Verato MDM Cloud™ creates one trusted identity for every patient and provider across an ACO, resolving records that originate in different organizations and different electronic health records into a single, governed view. It sits above existing systems rather than replacing them, enabling the population analytics, care coordination, and quality performance that shared savings models demand. Knowing Who Is Who™.