The Medicare login upgrade nobody's talking about: why identity infrastructure is the most underrated distribution rail in health tech

MAR 07, 2026 • PAID

Table of Contents

Abstract

Topic: CMS's March 2026 announcement adding CLEAR, ID.me, and Login.gov Medicare.gov is being read as a pedestrian security upgrade. It's actually a signal verified digital identity is becoming foundational infrastructure across the healt system, with massive downstream implications for startups, health system partnerships, and fraud prevention.

Key data points:

- Healthcare identity fraud costs over $5B annually; synthetic ID fraud up 311% Q1 2024 to Q1 2025

- DOJ's June 2025 healthcare fraud takedown charged 324 defendants tied to $1 in fraudulent claims

- ID.me: 157M total users, 80M verified to federal IAL2, 70+ healthcare orgs, $2 credit facility from Ares Management in Jan 2025

- CLEAR projected $2M in savings per 25,000 verified patients at Wellstar; digit check-in adoption jumped from 2% to 10%

- CLEAR1 integrates with Epic/MyChart out of the box; deployed at Wellstar, Ta General, Hackensack Meridian, Ochsner, and others

- ID.me 2024: 409M authenticated logins, up 44% YoY; 20.4M new wallets added

- The real play isn't better logins. It's a reusable, portable, IAL2-compliant ident layer that can power prior auth, claims adjudication, prescription access, clinica enrollment, and cross-entity data sharing

- The smart money isn't reading this as a cybersecurity announcement. It's a plat moment. The winners will be the companies that figure out how to build workfl on top of verified identity as infrastructure rather than treating it as a security checkbox.

What CMS Actually Announced (And W Everyone Glossed Over It)

On March 3, 2026, CMS dropped a fact sheet announcing that Medicare.gov wou now support three external login options for beneficiaries: ID.me, CLEAR, and Login.gov. The announcement reads like a press release written by someone whc primary goal was to put healthcare journalists to sleep. The language is exactly v you'd expect from a federal agency trying to explain something mildly complicat an audience it assumes has very low technical tolerance. Phrases like "enhanced

security," "protect your Medicare information," and "strict federal security stan
are doing a lot of heavy lifting. There's no mention of NIST 800-63-3 IAL2
compliance, no acknowledgment of what a reusable verified credential actually
enables downstream, and zero framing of why this matters beyond the obvious "
bad, security good" narrative.

So it's no surprise that most people in health tech saw this, nodded, and moved o
When the average digital health startup founder is heads down on product-mark
and the average health system CIO is still trying to get their EHR to stop crashir
Monday mornings, a Medicare login upgrade is not the thing that lights up the g
chats. It competes for attention against AI clinical documentation tools, the late
rate notice, and whatever CMS proposed rule dropped that week.

But pay attention, because this announcement is the visible tip of something mu
more interesting. It's the formal codification of what has been building quietly o
the past two years: a federated, government-backed identity verification layer is
installed across the largest healthcare payer in the country, and it's being built o
same commercial rails that already exist in the private sector. That's not a login
upgrade. That's infrastructure.

To understand why that matters, go back to December 2025. CLEAR announced
CMS contract first, framed explicitly under CMS Strategic Advisor Amy Gleason
Kill the Clipboard initiative, which is one of three named modernization priorit
CMS has set for Medicare. That framing is deliberate. Kill the Clipboard is not a
metaphor for reducing paperwork. It is a specific, named initiative to make patie
intake digital, portable, and interoperable. Gleason's quote at the CMS-CLEAR
hosted event in Washington was blunt: checking in at a doctor's office should fe
simple as boarding a flight. That's a CLEAR airport lane reference from the CM
strategic advisor. She knows exactly who she's partnering with and why.

ID.me announced its own CMS contract two weeks later. ID.me had been operati
under a broader HHS contract since 2022, but the explicit Medicare.gov expansi
new. Login.gov was already in the mix as the government-run alternative. So as o
early 2026, all three major government-grade identity verification providers are

officially plugged into Medicare, covering 67 million-plus beneficiaries who will increasingly authenticate through commercial identity wallets they can also use VA, SSA, and IRS.

Founders and investors who read this only as CMS worrying about fraud are mis the more interesting read, which is that CMS just created a standardized identit handshake that private-sector health companies can now build on top of. That's real story here.

The Identity Problem in Healthcare Is Way Bigger Than a Login Screen

To appreciate why verified identity infrastructure is such a big deal in healthcar specifically, it helps to understand just how broken the status quo actually is. Healthcare has been running on a comically insecure identity model for decades dominant paradigm for verifying who a patient is has historically been name, da birth, and the last four digits of a Social Security number. Sometimes a driver's l check at the front desk, which in practice amounts to a bored registration clerk glancing at a card before handing it back. It's the kind of identity verification th would make a mid-sized regional bank's compliance team genuinely upset.

The downstream consequences of this are substantial and well-documented. Healthcare identity fraud costs billions annually, and the problem has gotten dramatically worse as generative AI has made it cheap and fast to fabricate convi synthetic identities. A synthetic identity in this context is not a stolen real ident it's a fabricated one, assembled from fragments of real data and manufactured attributes, designed to pass through automated verification systems that are lool for red flags in known data rather than confirming the fundamental existence of person. Synthetic identity fraud in healthcare climbed hundreds of percentage p between 2024 and 2025, driven by AI tools that let bad actors create entirely fabricated identities complete with realistic documentation, digital footprints, a supporting records.

The DOJ responded to the growing fraud environment in kind. In June 2025, it announced what it described as the largest healthcare fraud takedown in history 324 defendants tied to more than $14 billion in fraudulent claims spanning telel scams, genetic testing fraud, durable medical equipment schemes, and synthetic identity abuse across Medicare and Medicaid. The government suspended billio pending payouts as part of that action. That number gets cited in press releases then forgotten. It shouldn't be. Fourteen billion dollars is not a rounding error. systemic failure of identity verification at scale.

The fraud problem, though, is actually the smaller part of the story. The bigger i is that the healthcare system has never had a trusted, portable, cross-entity way definitively say that this person is who they claim to be. It has had proxies. Insur cards. Medical record numbers. NPPES identifiers for providers. But none of th are identity-proofed to any meaningful standard, and none of them travel with a patient across the full care continuum in an interoperable way. The fragmentatic almost impressive in its thoroughness. A patient can walk into their primary car physician, their cardiologist, their pharmacy, and their payer's member portal ar have four completely different ways their identity is verified, stored, and manage with zero authoritative linkage between any of them. In any other industry that handles sensitive personal data, this would have been solved many years ago.

The operational consequences are real and measurable. Duplicate medical recor a pervasive problem across health systems. When a health system can't definitive link a patient across visit types and encounter modalities, it creates duplicate re which corrupt clinical data, generate incorrect medication histories, and create l errors that are expensive to unwind. In cases of actual medical identity fraud, st credentials end up embedded in the wrong patient's clinical record, including bl type, allergies, and medication lists, which is a patient safety problem on top of administrative one. The cost of resolving duplicate records, managing claim complications from mismatched identities, and processing fraudulent claims attributed to real beneficiaries adds up to a genuinely large number per health s per year.

What NIST 800-63-3 IAL2 actually means in practice is that someone has been verified against a government-issued document, a biometric liveness check, and authoritative data sources, meeting the federal standard for high-assurance iden is the same standard used for accessing VA benefits, IRS tax records, and SSA accounts. It is genuinely meaningful from a security standpoint, not the kind of compliance theater that health tech is unfortunately full of. The fact that this standard is now being formally applied to Medicare beneficiary access, through commercial providers who also serve dozens of private-sector healthcare organizations, is what creates the platform dynamic that makes this worth payin attention to.

CLEAR, ID.me and Login.gov: Not Just Gatekeepers, But Infrastructure

The airport-lane framing for CLEAR and the discount-verification framing for I dramatically undersell what these companies have actually built. Most of the hea tech audience knows CLEAR from TSA PreCheck comparisons and knows [ID.m (http://ID.me) from the IRS login chaos of 2021. Neither of those associations cap what these platforms look like in 2026.

CLEAR went public in 2021 and trades under the ticker YOU, which is either a corporate branding decision or the most optimistic ticker symbol on the New Yo Stock Exchange depending on how the stock is performing when you read this. T commercially interesting product for health tech purposes is CLEAR1, the enter identity platform that does biometric document verification, authoritative sourc corroboration, and liveness checks as an out-of-the-box identity and access management solution. The critical detail for anyone building on Epic is that CL integrates with Epic, including MyChart, without requiring a custom implemen project. That matters because Epic is the dominant EHR in hospital settings, co roughly 38% of U.S. hospitals and 35% of medical practices. An out-of-the-box CLEAR1 plug-in means any health system on Epic can deploy biometric check-i verified MyChart account access without a multi-year IT project and the associa organizational trauma.

CLEAR has moved quickly on health system partnerships. Wellstar Health Syste Georgia was the first to co-develop the CLEAR1 integration and went live with biometric check-in kiosks across medical office locations. The results from the Wellstar deployment are concrete: digital check-in adoption climbed from 2% to after launch, 73% of patients who used the system said they would use it again, a linking appointments to a verified identity, Wellstar uncovered and resolved dup patient records before visits, with projected savings of roughly $2 million for eve 25,000 patients verified. That's approximately $80 per patient in administrative savings from cleaner records alone, before accounting for fraud prevention or re registration staff time. The math scales quickly across a large health system. Bey Wellstar, CLEAR has signed partnerships with Tampa General Hospital, Univer Miami Health, Hackensack Meridian Health, Community Health Network, and Ochsner Health, and is working toward a deeper MyChart integration for patien portal access beyond the check-in use case.

The Tampa General deployment is worth noting separately because it extends th case into workforce identity. CLEAR deployed its biometric identity platform fo clinical staff at Tampa General, cutting MFA reset times from days to minutes a establishing a verified credential baseline for provider access management. The workforce use case is underappreciated in discussions about identity infrastruct healthcare. Clinician credential verification, provider access management for EH systems, and staff identity for cross-departmental access are substantial operatic problems that currently get handled through a mix of password managers, help d tickets, and IT contractors. A biometric identity layer for clinical workforce tha travels across health systems would reduce both administrative overhead and the of credential fraud that shows up in healthcare workforce infiltration schemes.

ID.me is a structurally different story and arguably the more interesting investm narrative. The company has taken a wallet-first approach, building a reusable ve credential that a user completes once and then uses across any ID.me-connected entity, currently spanning 20 federal agencies, 45 states, 70-plus healthcare organizations, and more than 600 private-sector brands. In 2024, the platform ac more than 20 million new wallets and supported 409 million authenticated login

44% increase year-over-year. By late 2025, ID.me reported 157 million total users 80 million verified to the federal IAL2 standard. The revenue model is per-verifi fees and subscription arrangements that compound over time because a verified credential gets reused across all connected entities, meaning revenue from the ir verification multiplies as the user accesses different services. Ares Management committed a $275 million credit facility to the company in January 2025, with a planned equity component as well, so the capitalization story is solid.

The more interesting strategic signal from ID.me is its explicit intent to move up value chain beyond authentication. The company has been publicly clear that it s its wallet as a vehicle for identity-mediated data exchange, not just secure login. partnership with Flexpa, announced in late 2025, specifically positioned ID.me a enabler of patient-controlled data flows and marked the first connection betwee digital credential service provider and the TEFCA framework. TEFCA is the Tru Exchange Framework and Common Agreement that CMS has been building as t backbone for nationwide health information exchange. Being the first commerci identity provider to plug into TEFCA as an identity anchor is not an accidental partnership. It's a deliberate move to become the identity layer through which patient-controlled data sharing flows, positioning the wallet as something that s upstream of the data exchange rather than just beside it.

Login.gov is the government-operated option and the least commercially interes of the three for startup purposes. Its importance is primarily political: it gives beneficiaries who prefer not to use biometric facial recognition with a private company a government-run alternative, which is necessary for the CMS announcement to survive the civil liberties scrutiny that tends to follow federal biometric programs. It also creates a competitive check that keeps ID.me and CI from having unchallenged pricing power in the government segment. For health founders thinking about building on top of this infrastructure, Login.gov is prol not the primary integration target, but its existence as an option matters for the durability of the whole system.

The Kill the Clipboard Play: What This Signals for the Market

Kill the Clipboard, as a named CMS initiative, is worth taking seriously as a mar signal even if the branding sounds like a campaign from a medical office supplie company trying to pivot to software. It sits alongside two other named moderniz priorities within CMS's Health Tech Ecosystem Initiative, which is structured as voluntary ecosystem where private companies pledge alignment with CMS interoperability priorities and commit to building products that enable modern Medicare experiences. Louisiana became the first state to formally join the initia and CMS has indicated that other states can now take the pledge. The early commercial contracts with CLEAR and ID.me are the first concrete outputs of th initiative with real dollar values attached.

The structure of the initiative matters for health tech founders. Because it's a voluntary commercial ecosystem rather than a traditional government procurem program, companies building on it retain commercial flexibility that would be constrained under a federal contract vehicle. The identity layer being installed is commercial-grade, not government-specific, which means private-sector compar can build on top of these platforms without needing a federal contracting relatic themselves. The Epic integration angle means the primary distribution path run through commercial health system channels that health tech companies already how to navigate, rather than through government procurement pathways that re very different organizational capabilities and sales cycles.

The CMS announcement also mentioned explicitly that the CLEAR and ID.me deployments will be used for the forthcoming National Provider Directory for Medicare providers. That is provider-side identity, not just patient-side, and it's deal. A verified provider identity layer that travels across Medicare, Medicaid, ar eventually commercial payers would fundamentally change the infrastructure fo credentialing, prior authorization, telehealth, and care navigation. If a provider's identity can be verified once at IAL2 and that credential is reusable across payer platforms, the entire credentialing workflow changes in ways that benefit both h

systems and the vendors building around them. CAQH, the industry utility that currently handles much of the provider data standardization burden, processes credentialing information for more than 2 million providers. A verified, portable government-anchored provider identity layer creates a competitive pressure on t model that hasn't existed before.

The signal worth tracking alongside this announcement is the administration's broader posture toward digital identity infrastructure. The initiative aligns expl with what has been called the interoperability goals of the current administratio connecting to prior efforts around patient data access, provider directory standardization, and the 21st Century Cures Act information blocking rules tha been accelerating health data portability. Identity is the layer that makes all of t data portability work in practice. Rules that require data sharing only matter if y can verify who is authorized to request and receive the data. Verified identity at applied consistently across the ecosystem, is the technical precondition for interoperability working the way its proponents intend.

Creative Use Cases Nobody Is Building Yet (But Should Be)

Most people in health tech, when confronted with this announcement, think fra prevention and patient access. Those are real use cases and worth building. But they're also the obvious ones, and obvious use cases in health tech tend to be wh the first wave of startups goes to get squeezed by incumbent players who eventu build or buy their way in. The more interesting opportunities are in the adjacent applications that a verified, portable, government-grade identity layer makes pos for the first time at scale.

Prior authorization is the most immediate and highest-value adjacent use case. F one of the most operationally broken workflows in American healthcare, consum roughly $13 billion annually in administrative costs by standard industry estima The current workflow requires verifying that the right provider is requesting th service for the right patient with the right clinical documentation. All of that

verification currently happens through a combination of fax, web portals, and pl trees where the identity of the requesting provider is essentially never verified to meaningful standard at the front of the process. It's verified in the sense that son entered credentials into a payer portal, not in the sense that those credentials ha been validated against authoritative sources. A verified provider identity at IAL2 linked to a portable credential that travels across payer systems, changes the authorization workflow structurally. Automated, pre-verified PA routing become technically feasible in a way it hasn't been before, because the identity of the requester is trusted at the intake rather than assumed or manually reviewed midstream. The payer-side efficiency gains from reducing manual identity reconciliation in the PA process are substantial, and the provider-side reduction administrative burden is even larger.

Prescription drug access, specifically for controlled substances via telehealth, is another enormous application. The Drug Enforcement Administration has been wrestling with telehealth prescribing rules for controlled substances since pand era flexibilities began expiring, and the policy back-and-forth has created signifi uncertainty for telehealth platforms and their clinical partners. The core regulat concern underneath all of that policy debate is identity verification: is the patien they claim to be, is the prescribing provider licensed in the relevant state, and is prescribing encounter genuine rather than manufactured. All three of those que have substantially cleaner answers if the participating parties are verified at IAL through a trusted commercial provider before the encounter even begins. A com that builds a DEA-compliant telehealth prescribing workflow on top of an existi IAL2 identity layer has a regulatory moat that is genuinely difficult to replicate because it's anchored in a federal compliance standard rather than a proprietary technical approach.

Clinical trial enrollment is a particularly underrated application and one where identity problem is almost never discussed in startup pitches despite being a significant cost driver. Clinical trials spend a substantial portion of their screeni and enrollment budgets on patient eligibility verification and consent manageme meaningful share of that cost is identity-related: confirming that the patient is w

they say they are, that their consent is genuine and informed, and that their self-reported eligibility criteria actually match their verified health history. Digital t platforms that integrate verified identity at the enrollment stage could materiall reduce screen failure rates and consent irregularities, while also making remote participation more credible to FDA reviewers who have historically been skeptic non-in-person enrollment. The FDA has been expanding its guidance on decentr clinical trials, and verified digital identity is a prerequisite for that expansion to at scale in a way that generates trustworthy data.

Dual-eligible care navigation is a sleeper use case that deserves more attention f founders building in the complex care space. Dual-eligible beneficiaries, people qualify for both Medicare and Medicaid, interact with multiple payers, multiple providers, and multiple government programs across their care journeys, and th verify their identity at essentially every touchpoint. If a verified identity credent travel with a dual-eligible beneficiary from their PCP to their behavioral health provider to their pharmacy to their DME supplier to their managed care organization's member portal, the care coordination implications are real. Care coordinators can authenticate patients remotely with confidence. Benefits eligib can be checked in real time at the point of care without the call-center loop. Soc services referrals can be made with a trusted identity anchor that doesn't requir patient to prove who they are from scratch at each social service organization th interact with. For a population that is disproportionately elderly, low-income, ar often cognitively complex, reducing that identity friction has both operational a clinical value.

Workforce credentialing for clinical staff is the B2B version of all of the above a probably the fastest path to revenue for a well-positioned startup. The Tampa G deployment is the proof point that this market exists and is willing to pay. Clini MFA resets, EHR access provisioning, traveling nurse credentialing verification, locum tenens identity management are currently handled through processes tha simultaneously burdensome and insecure. A biometric identity layer for clinical workforce that is interoperable across health systems would reduce administrati overhead, reduce the window for credential fraud, and create a portable professi

identity that clinicians can carry from one employer to the next rather than re-credentialing from scratch at each new affiliation. The traveling nurse and locur physician markets alone represent significant addressable revenue given the ong staffing volatility in hospital systems.

The attribute-sharing use case is the longest-duration play and potentially the m structurally valuable. Once a large population is verified at IAL2, that verified id becomes a trusted anchor for sharing specific attributes without sharing the underlying identity itself. Coverage status verification in real time at the point o Disability determination confirmation for accommodation requests. Income verification for subsidy eligibility calculations. Veteran status confirmation for discount and benefit programs. Student enrollment confirmation for educationa discount programs at health systems. All of these currently require manual docu submission, call-center verification, or third-party data vendor relationships tha introduce latency and error rates. An IAL2-anchored attribute-sharing model th a patient authorize specific disclosures from their verified identity without shari the full record is the technical architecture that makes a genuinely patient-contı health data ecosystem work in practice rather than just in policy documents.

What This Means for Investors and Founders

The investment thesis that flows from all of this is not simply "buy ID.me and C stock and wait," though the unit economics of reusable verified credentials compounding across a growing network of connected entities are worth understanding as a comparable for what the platform layer ultimately looks like healthcare. The more interesting investment angle is in the companies that build top of this infrastructure in workflows where verified identity unlocks somethin wasn't previously technically or commercially feasible.

The characteristics of startups most likely to win in this space share a few patter The first is deep payer or health system channel relationships, because the distribution of identity infrastructure in healthcare runs through those instituti

and the companies with embedded relationships will move faster than those tryi
sell to the same institutions from a standing start. The second is workflow speci
the companies that pick one high-value workflow like PA or controlled substanc
prescribing and go deep on the identity-enabled version of that workflow will
outperform the ones trying to build a general-purpose identity layer on top of id
layers that already exist. CLEAR and ID.me are the platform; the opportunity fo
startups is in the applications. The third characteristic is regulatory fluency. The
reason the DEA prescribing use case and the FDA decentralized trial use case ar
interesting is precisely because the regulatory complexity creates a barrier that s
down generalist competitors. Founders who understand the specific regulatory
requirements around identity verification in their target workflow have a durabl
advantage that pure technology capabilities don't replicate.

The risk factors worth taking seriously are the ones that apply to any play that
depends on government infrastructure. The Kill the Clipboard initiative exists v
an administration that has both appetite for this kind of modernization and a tra
record of implementing policy changes that create second-order disruption to
established healthcare technology businesses. If the political winds shift and the
voluntary ecosystem structure changes, the commercial terms for companies tha
built distribution through CMS alignment could change too. The mitigation is
obvious in theory and hard in practice: build products that deliver enough stand
value that the government alignment is an accelerant rather than the entire busi
model.

The access equity issue is real and worth taking seriously both as a policy matter
as a market design problem. The concern that cognitively impaired elderly
beneficiaries, those without smartphones, and those with limited digital literacy
find IAL2 verification burdensome is legitimate. CMS has attempted to address
with in-person verification options, phone assistance, and public computer acces
the fact that Login.gov exists as a government-run non-biomet
alternative matters for this population. But the founders who figure out how to m
IAL2-grade verification accessible to the hardest-to-reach beneficiaries, whether
through assisted digital workflows, caregiver delegation with appropriate

authorization constraints, or offline verification pathways that feed into the sam trusted credential, are solving a problem that CMS actively needs solved and tha pure digital-first players have not addressed well.

The bottom line for the health tech investment community is this: verified digita identity is transitioning from a compliance checkbox to a distribution rail. The companies that recognize it as infrastructure and build on top of it accordingly v have access to workflows, data flows, and commercial relationships that the com treating it as a security feature will not. The CMS announcement in March 2026 interesting because of what it says. It is interesting because of what it makes pos that wasn't possible before, and because the federal government just made the b public enough that the market has to respond.

3 Likes

← Previous

Nex

Discussion about this post

Comments Restacks

Write a comment...