



A GOVERNMENT TECHNOLOGY THOUGHT LEADERSHIP PAPER

Why Identity Is Now Core HHS Infrastructure

Modern identity solutions are key to service access and program integrity.



SPONSORED BY



Health and human services agencies face mounting pressure to protect program integrity, reduce improper payments and deliver a low-friction experience for eligible beneficiaries. At the same time, sophisticated fraud attacks are using AI and automation to target critical benefit programs, including Medicaid and the Supplemental Nutrition Assistance Program (SNAP).

These pressures create a new reality for HHS agencies: Identity verification is no longer a supporting function. It's core infrastructure that affects who can access services, how confidently agencies can verify continued eligibility, and how effectively they can prevent improper payments and fraud.

Modern identity infrastructure gives agencies a consistent, risk-based way to verify new applicants and returning beneficiaries. Instead of relying on static checks or siloed tools, agencies can use adaptive controls to detect fraud earlier, reduce manual review and improve confidence in eligibility-related decisions.

Key Challenges for HHS Agencies

Congress passed H.R. 1 in 2025, significantly changing the operating environment for multiple HHS-related authorities. SNAP agencies, for instance, must reduce application payment error rates below 6% by 2028 or face financial consequences. Some Medicaid recipients must go through redetermination or recertification twice a year instead of annually.

Strengthening error prevention can reduce both the fiscal impact of improper payments and the reputational damage caused by error-prone systems. However, stricter federal eligibility requirements and heightened payment scrutiny also raise the stakes for HHS agencies. More frequent recertification increases verification volume and creates additional opportunities for fraud. Meanwhile, AI-driven attacks are making it easier for fraudsters to exploit weaknesses in recertification workflows.

The following challenges underscore why identity must be treated as foundational infrastructure for payment accuracy, fiscal stability and public accountability:



At-risk users. SNAP and Medicaid program applicants must show they qualify for benefits. This starts with digital identity verification. But individuals applying for these benefits often lack a typical financial footprint, so credit bureau-based solutions fall short in verifying this population.

"Traditional identity verification solutions rely heavily on credit header data," says Will Kern, a principal solutions consultant at Socure. "As a result, they miss out on a large demographic typically served by these benefits programs."

Applicants may lack a permanent home address. They may rely on prepaid phones or apply for benefits on a public computer at the local library, which can trigger fraud alerts in legacy verification processes.

"High-risk signals like library computers and prepaid phone numbers may be evidence of fraud, but they're also evidence of your normal user base," says Neal Gallucci, head of public sector solution consulting at Socure.

Ensuring equitable access means addressing these issues in a way that balances access and program integrity. Policies designed to foster inclusiveness may misfire, however, by removing obstacles for fraudsters who can easily circumvent obsolete tools and processes.



Why IAM Platforms Aren't Enough

Identity and access management (IAM) platforms are crucial components of identity infrastructure, but they have limitations when it comes to mitigating fraud.

Strong for ongoing account access: IAM platforms are essential after account creation because they protect credentials, enforce access controls and authenticate original account holders so they can securely access services over time.

Limited at account creation: IAM solutions typically lack purpose-built capabilities to verify whether an individual is truly who they claim to be during account creation. IAM tools authenticate credentials, not the underlying real-world identity.

The fraud gap: Without dedicated identity verification and adaptive fraud risk assessment at onboarding and recertification, agencies risk creating windows for fraud. Under H.R. 1's expanded verification cadence and heightened payment scrutiny, this gap directly amplifies improper payment exposure.

Evolving fraud threats. Large volumes of personally identifiable information (PII) are available on the dark web. Legacy verification methods like knowledge-based authentication (KBA) — which requires users to recall relatives' names, former addresses and other personal details — are obsolete because criminals can easily find this information online.

Fraudsters armed with this data and AI/ML tools can attack at scale, driving program costs higher at a time when cost controls are critical. When budgets are tight, fraud diverts money from people who need it.

Gallucci says agencies traditionally budget for a small volume of fraud, making a tradeoff to ensure access. However, AI-driven fraud can blow up an agency's budget.

"It's worth it to be right 97% of the time because making sure a child doesn't go hungry is more important," he says. "But that 3% fraud rate can become a 15% fraud rate you didn't budget for, and now you're low on funds because you improperly distributed them."

Growing verification volume. Verifying beneficiaries more frequently creates more potential entry points for fraud and increases the pressure for manual reviews. Agencies that lack modern, adaptive identity

controls face a difficult choice between tightening controls and overwhelming staff capacity or loosening controls and accepting higher improper payment rates.

Fragmented identity across programs. Medicaid, SNAP and similar programs often operate on disconnected or siloed identity systems. "They may have a device-reputation solution that doesn't talk with their third-party fraud solution," Kern says. Fraudsters exploit these kinds of gaps.

As eligibility requirements become more rigorous and cross-program data matching increases, fragmented identity systems introduce duplicate records, data mismatches and inconsistent validation outcomes. Without a unified identity layer, agencies face more manual rework, less confidence in eligibility decisions and greater risk to program integrity, even when applicants are acting in good faith.

Moreover, improper payments don't always result from flawed eligibility logic or outright fraud. Many mistakes stem from ambiguous identity signals at onboarding or renewal. If identity confidence is inconsistent, downstream controls like income matching, cross-program validation and duplicate detection become unstable.



Modernizing Identity Infrastructure

Key advantages of a modern identity infrastructure include:

Dynamic risk scoring. AI-enhanced platforms integrate identity intelligence in real time from onboarding through recertification. The software evaluates dozens — or even hundreds — of user, device and transaction behaviors and gives each one a score that synthesizes risk. “The passive, risk-based solution runs in the background,” Kern says. “The applicant doesn’t know it’s happening.”

This type of solution lets agencies get the right benefits to the right individuals at the right time. Socure’s software, for instance, uses real-time, risk-based scoring that approves up to 98% of applicants and requires extra verification only when it identifies measurable risk.

Holistic, user-centric experience. Risk-based verification can layer with identity and access management (IAM) tools, ensuring comprehensive program integrity that continuously verifies identity in the background. Agencies can deliver a seamless digital journey, preventing fraud while making it easy for people to engage with their services.

Statistical modeling and continuous feedback let agencies adjust friction based on evidence of risk. Low-risk applicants can be approved with ease, while higher-risk applicants can be required to provide additional information and/or documentation. This flexibility allows agencies to minimize burden while targeting potential fraud with precision and clarity.

3 Types of Digital Fraud

Identity-based fraud usually falls into these categories:

First-person: Applicants use their own identity to access benefits programs they do not qualify for. The primary risk here is someone using their identity across multiple state benefits systems. While first-person fraud is important to consider, the damage usually is limited because the applicant has only one genuine identity, which makes it difficult to scale first-person fraud attempts.

Synthetic: Fraudsters use AI to create large volumes of phony applications with fake personal data. States have implemented digital identity controls that can combat synthetic fraud effectively, which motivates criminals to find weaker targets.

Third-person: Fraudsters steal PII via phishing or buy it on the dark web. They use real PII for account takeovers that divert money to accounts they control. AI/ML tools make it easier to mount third-party attacks at scale, which makes this fraud the most prevalent identity risk for agencies providing public benefits.

Higher agency productivity. By preventing fraud at the front door, agencies gain time downstream. Risk-based identity verification weeds out fraudulent identities so you can have confidence that you are conducting eligibility checks on real, verified individuals. “You’re increasing program integrity while reducing worker caseload,” Kern says. “You’re not wasting time doing employment and income verifications on stolen or synthetic identities.”

Automated risk scoring also reduces false positives that drive administrative rework and undermine payment accuracy as eligibility standards tighten. Common actions like account recovery, credential management and profile updates can be automated through configurable workflows, boosting operational efficiency while maintaining strong compliance and risk reduction.

Applying real-time risk scores at each interaction minimizes unnecessary escalations.

Secure self-service capabilities. Modern platforms use low/no-code interfaces that let business users adapt the software to specific needs without assistance from central IT authorities. “Something that may have taken weeks or months can now be done by business analysts in real time so you can see benefits immediately,” Kern says.

Forensic tools. Identity analysis detects synthetic identities, anomaly clusters and coordinated fraud patterns. Establishing this baseline helps agencies quantify fraud exposure, identify identity-related vulnerabilities and respond faster.

Defensible audits. Under heightened federal scrutiny, agencies must demonstrate outcomes and explain how decisions were made. Advanced identity platforms provide traceable validation steps, documented risk scoring and reproducible decision logic tied to eligibility determinations. This defensible audit trail strengthens oversight while reinforcing measurable payment accuracy.

Managing Eligibility Complexity

More rigorous eligibility rules raise the cost of inaccurate benefits determinations. While technology can ease cost pressures, controls must be used with care. Blanket documentation requirements and uniform verification controls can be counterproductive if they raise friction for users, increase application abandonment and expand administrative rework.

Uniform controls also incentivize fraudsters to create automated attacks on predictable checkpoints. Targeted, risk-based controls shift this dynamic by adding user friction only where risk justifies it.

These tips will help agencies get the best performance from a modern identity infrastructure:

Establish a baseline with a forensic portfolio scrub.

Conduct a comprehensive forensic analysis of your user base to understand your true fraud footprint. Identify troubling trends, anomalous patterns,

synthetic identities and potential organized fraud groups. This data-driven baseline provides visibility into your current risk exposure and creates a compelling foundation for modernization.

Implement real-time risk assessment and segmentation. Use insights from the forensic scrub to design a real-time risk-mitigation strategy. Apply identity and behavioral signals at each interaction to evaluate risk and direct applicants to the right level of verification.

Manage risk dynamically. Route higher-risk applicants through enhanced verification workflows; lower-risk applicants can usually be approved passively. Guard against overaggressive controls that increase false positives, leading to delayed benefits, appeals and erosion of public trust. Dynamic risk management concentrates friction where risk signals justify it, reducing unnecessary denials and stabilizing payment accuracy under evolving eligibility standards.

Continuously monitor, measure and adapt. Use performance analytics and feedback loops to track fraud capture rates, false positives and user experience metrics. Ongoing monitoring lets agencies dynamically adjust automated decisioning, refine risk thresholds and respond quickly to emerging fraud patterns.

Protecting Vulnerable Populations

Modern identity infrastructure makes it easier to get people the help they need while giving HHS agencies the foundation to prevent increasingly sophisticated fraud and the flexibility to adapt to shifting verification requirements.

Fraud prevention must be continuous. Attacks are becoming faster, more automated and more adaptive.

“Fraud will adjust as you apply friction,” Gallucci says. “Modern identity verification platforms use real-time risk scoring and behavioral signals to help agencies identify new fraud tactics early and adjust controls accordingly.”



This piece was written and produced by the Government Technology Content Studio, with information and input from Socure.



Produced by Government Technology

Government Technology is about solving problems in state and local government through the smart use of technology. Government Technology is a division of e.Republic, the nation's only media and research company focused exclusively on state and local government and education.

www.govtech.com



Sponsored by Socure

Socure is the leading platform for digital identity verification, compliance and fraud prevention solutions, trusted by the largest enterprises and government agencies to build trust and mitigate risk. Leveraging AI and machine learning, Socure's industry-leading platform achieves the highest accuracy, automation and capture rates in the industry. Serving more than 3,000 customers and 190+ countries across financial services, government, gaming, healthcare, telecom and e-commerce, Socure's customer base includes 18 of the top 20 banks, four of the Mag 7, the largest HR payroll and workforce providers, the largest sportsbook and prediction market operators, 130 organizations across the public sector, and more than 600 fintechs. Leading organizations trust Socure to deliver certainty in identity across onboarding, authentication, payments, account changes and regulatory compliance.

www.socure.com