CMS IDea Challenge Event Summary: Strategies for Securing Member IDs

CMS IDEA CHALLENGE OVERVIEW

In December 2025, the CMS Center for Program Integrity (CPI) hosted the **CMS IDea Challenge**, a series of two in-person, solution-oriented events designed to generate **actionable ideas to address member ID and Medicare Beneficiary Identifier (MBI) theft and misuse**.

The events began with remarks from CMS leaders and an **overview of member IDs and fraud threats and vulnerabilities** related to their theft and misuse. Then, attendees worked in teams to **identify a top problem** with member ID theft and misuse and to **develop a pitch** to address their top problem.

ATTENDEE REPRESENTATION

The events convened **78 total attendees**. Most common organization types were:

- Technology/Cybersecurity **(32)**
- Government Contractor **(14)**
- Health Care **(7)**

Attendees represented **41 different role types.** Most common role types were:

- Executive **(12)**
- Director **(12)**
- Program Manager **(7)**

Attendees came from **26 states**. Attendees most commonly came from California **(19)**, Maryland **(10)**, and New York **(8)**.

FRAME THE PROBLEM: DISCUSSION THEMES

During group working sessions, attendees discussed problems related to member ID theft and misuse. The following themes were common.

Exposed and Easily Accessible Data

- Broad access to MBIs and National Provider Identifiers (NPIs) increases the risk of theft.
- Limited controls over the data flows between payers, providers, and intermediaries and a lack of industry-wide layered authentication measures and access controls.
- Provider and member-service verification processes lack layered authentication measures (e.g., multi-factor authentication, biometric authentication).
- Inadequate internal controls on staff access and credential handling within providers enable internal fraud and data breaches.

Exploitation of Provider Enrollment Processes

- Fraudsters use false or misleading information to obscure ownership and the relationships between providers and suppliers, allowing them to evade detection
- Limited use of advanced checks for providers allows high-risk individuals to enroll.

Delays Between Service and Claims Submission

- Limited real-time authentication at the point of service or sale, combined with extended billing windows, make it harder to prevent fraud.
- Delayed audit findings reduce the timeliness and effectiveness of information sharing across the industry.

CMS IDea Challenge Event Summary: Strategies for Securing Member IDs

IDENTIFY A SOLUTION: DISCUSSION THEMES

During group working sessions, attendees discussed ideas related to addressing member ID theft and misuse. The following themes were common.

Dynamic Identity Security

- Augment or replace static identifiers (e.g., MBIs, NPIs) with provider- or claim-specific tokens that may only be valid for a single transaction or limited time, reducing risk if an identifier is compromised.

Dynamic Transaction Security

- Implement multi-factor authentication (MFA) and dynamic authentication for all system access and claims activities using methods like PINs, biometrics, and real-time alerts.

Robust Provider and Credential Management

- Strengthen provider enrollment screening by implementing stronger provider identity verification and performing additional screening checks using financial information, credit scores, and other available data.
- Leverage provider risk scores prior to enrollment and dynamically update them on an ongoing basis, denying access to the riskiest providers.

Enhanced Activity Monitoring

- Deploy transaction-level dynamic risk scoring, automatically flagging and prioritizing suspicious activity for immediate review, holding payments provisionally or re-issuing credentials when risks are elevated.
- Augment current claims monitoring processes with transaction metadata (e.g. transaction velocity, device type, device ID) to help identify potentially fraudulent claims.
- Enable rapid intervention with automated alerts, suspension protocols, and frequent reassessment of user access, helping to contain emerging threats before they result in fraud.

Beneficiary Notification, Transparency, and Engagement

- Use mobile apps or alerts to notify beneficiaries of suspicious claims and empower direct reporting of suspicious claims.
- Engage beneficiaries in the verification process by asking them to confirm whether certain easy-to-understand services took place and streamline methods for beneficiaries to review or report suspicious claims.

CMS IDea Challenge Event Summary: Strategies for Securing Member IDs

TOP VOTED CONCEPTS ACROSS IN-PERSON EVENTS

Teams presented ("pitched") their ideas. Then, attendees voted on their top pitches, considering potential effectiveness, feasibility, and user-friendliness. Below are summaries of the **top-voted concepts** per event.

SAN FRANCISCO, CA

Top-Voted Idea: Identity Binding and Real-Time Verification Framework

Challenge: The current system of static MBIs enables bad actors to continuously exploit compromised MBIs for fraud. Inadequate verification and lax oversight allow for stolen MBIs to be misused and for patient and program security to be compromised.

IDea: This solution introduces a dynamic Identity Binding and Real-Time Verification Framework that replaces static MBIs with unique, transaction-based IDs. This would verify both beneficiaries and providers using digital credentials and biometrics. This solution also provides real-time alerts and monitoring for proactive, risk-based fraud prevention. This would dramatically strengthen Medicare program security while streamlining the user experience. By empowering beneficiaries to pre-authorize high-risk services and requiring time-limited provider billing keys, the framework minimizes fraud opportunities and gives users greater control over their health care interactions.

Second Top-Voted Idea: Provider/Beneficiary Authentication at the Point of Service

Challenge: Without real-time verification of beneficiary-provider relationships at the point of service, Medicare is exposed to unauthorized claims and increased fraud risk. This vulnerability enables bad actors to exploit the system before fraud can be detected or stopped.

IDea: This solution authenticates both providers and beneficiaries at the point of service using National Institute of Standards and Technology (NIST) Identity Assurance Level 2 (IAL2) digital credentials, creating a unique transaction ID recording each verified encounter. An integrated API manages secure ID generation and digital exchanges, while beneficiaries receive real-time alerts and access details through a user portal. This aims to ensure only legitimate, authenticated claims are submitted.

NEW YORK, NY

Top-Voted Idea: Provider Verification and Per-Provider Unique Tokens

Challenge: A significant portion of provider enrollments are performed via paper filing, making it difficult to perform sophisticated identity verification. MBIs are universal keys, and CMS cannot currently identify the point at which MBIs are compromised.

IDea: This solution mandates electronic provider enrollment and multi-factor and biometric authentication to verify provider identities. To submit a claim, the verified provider would receive a private key. NPIs and MBIs are combined and cryptographically locked using the private key, creating a unique token in place of the actual MBI. This enables rapid breach containment and response by isolating risk to individual tokens, while safeguarding universal beneficiary information and seamlessly integrating with claims and eligibility systems.

Second Top-Voted Idea: Secure Provider/Beneficiary Exchange at the Point of Care

Challenge: MBIs currently lack user verification. This allows anyone with access to MBIs to use them. The absence of authentication creates a significant vulnerability, enabling widespread fraud if MBIs are stolen, copied, or misused.

IDea: The solution introduces a secure, cryptographic exchange between patients and providers at the point of care, producing a single-use, verifiable token for each Medicare claim. This process would start each claim with confirmed patient and provider identities, using multifactor authentication and credential checks. By requiring a unique, CMS-issued token for every encounter, only verified, face-to-face services can generate valid claims. This would improve auditability and significantly reduce fraud risk.