DEPARTMENT OF HEALTH & HUMAN SERVICES

Centers for Medicare & Medicaid Services
7500 Security Boulevard, Mail Stop 00-00-00
Baltimore, Maryland 21244-1850

Center for Consumer Information and Insurance Oversight
RELEASED: August 3, 2026

EDE Change Request (CR) 109: Identity Proofing and Agent/Broker Authorization

The Centers for Medicare & Medicaid Services (CMS) is committed to protecting consumers from unauthorized activity by bad actors. CMS's Federally-facilitated Exchanges (FFE) platform, including State-Based Exchanges on the Federal Platform (SBE-FP), serves as the individual market health insurance Exchange in 29 states. Since 2019, agents, brokers, and web brokers have used Enhanced Direct Enrollment (EDE) technology platforms to submit eligibility applications and to enroll consumers in coverage. Most consumers who enroll in coverage through the Health Insurance Marketplace are assisted by an agent, broker, web broker.[1][2] Despite existing consumer identity proofing requirements, EDE partner platforms historically have varied in how they operationalize identity proofing and agent/broker authorization. These gaps have created opportunities for bad actors to enroll unaware consumers ("unauthorized enrollments") or change consumer plans without authorization ("unauthorized plan switching"). CMS has previously taken steps to prevent unauthorized plan switching.[3]

CMS is taking additional steps to bolster program integrity in the Health Insurance Marketplace and crush fraud by issuing new requirements that aim to reduce unauthorized enrollments. On May 27, 2026, CMS announced a change request[4] that requires EDE partners operating on the FFE to systematically enforce consumer ID proofing and agent/broker/web broker authorization for applications or enrollments submitted through the EDE agent/broker pathway. These changes will be in place for all applications submitted through the EDE agent/broker pathway ahead of Open Enrollment Period (OEP) 2027. This FAQ document addresses some common questions regarding this change.

---

[1] Approximately 76% of active plan selections for Open Enrollment 2026.

[2] EDE is a service that allows approved QHP issuers and third-party web-brokers (online insurance sellers) to enroll consumers in Exchange coverage, with or without the assistance of an agent/broker, directly from their websites. It provides a comprehensive consumer experience including the eligibility application, Exchange enrollment, and post-enrollment year-round customer service capabilities for consumers and agents/brokers working on behalf of consumers, directly on issuer and web-broker websites. Through EDE, approved EDE Entities build and host a version of the HealthCare.gov eligibility application directly on their websites that securely integrates with a back-end suite of FFE application programing interfaces (APIs) to support application, enrollment and more.

[3] July 2024: *CMS Statement on System Changes to Stop Unauthorized Agent and Broker Marketplace Activity*

[4] Pursuant to *Year 9 Guidelines for Third-party Auditor Operational Readiness Reviews for the Enhanced Direct Enrollment Pathway and Related Oversight Requirements - PY 2026 and PY 2027*, CMS periodically releases new requirements and updates to existing program requirements in the form of "CMS-Initiated Change Requests." All EDE partners must implement CMS-initiated Change Requests upon CMS-defined timelines and submit documentation to demonstrate their compliance with new/updated requirements.

Note: This document uses the abbreviation "AB" or "ABs" to refer to agents, brokers, or web brokers who assist consumers through EDE partner platforms. This document also uses the abbreviation "A/B pathway" to refer to the pathway used by agents, brokers, or web brokers to enroll consumers through the EDE partner platforms.

Q1: What are the new EDE requirements announced by CMS on May 27, 2026?
A1: In preparation for Open Enrollment for 2027, EDE partners must systematically enforce consumer identity proofing and get AB authorization from the consumer for applications or enrollments submitted through the EDE A/B pathway. EDE partners must implement changes based on the risk-based framework prescribed by CMS.[5]

While each EDE partner implementation of these requirements may differ from EDE platform to platform, all EDE partners must implement these changes based on technical requirements published by CMS. For certain applications that meet "high risk" criteria, the household contact/application filer must first be identity proofed prior to collecting AB authorization. All applications will require AB authorization regardless of risk criteria. ABs will be blocked from proceeding through the application and/or enrollment process without AB authorization. These changes are scheduled to go into production on EDE partner platforms no later than **October 12, 2026**.

Q2: What are the risk criteria prescribed by CMS?
A2: Applications or enrollments that meet any of these conditions are considered "high-risk":

- New consumer applications, including applications submitted for consumers seeking coverage in a different coverage state;
- Consumer applications with at least one active enrollment, not including stand-alone dental plans, that have a net premium amount (after Advance Payments of Premium Tax Credits (APTC)) of $30 or less per month;
- Consumers working with a different or new AB.

All other applications and enrollments that do not meet "high-risk" conditions are considered "low-risk". For all "low-risk" applications and enrollments, EDE partners must require a lightweight mechanism (such as a one-time passcode or a one-time confirmation link) to capture AB authorization from the consumer to allow an AB application or enrollment action on the consumer's behalf. There may be scenarios where an application or enrollment move between "high-risk" and "low-risk" categories. Examples include consumer applications with existing enrollments excluding stand-alone dental plans (SADP), that have net premium amounts (after APTC) greater than $30 per month, or consumers working with the same or previously authorized AB. CMS expects EDE partner platforms to appropriately require identity proofing whenever an application fit the "high-risk" criteria.

[5] These requirements will not replace the existing requirement for ABs to obtain consumer "consent" which is required per 45 CFR 155.220(j)(2)(iii). See Question 7 of this FAQ document.

Q3: How will EDE partner platforms communicate with consumers and collect identity proofing and AB authorization information?
A3: EDE partners may use text messages, emails, or automated phone calls to contact consumers (using the contact information on the application for existing applicants or newly collected information for new applicants) for purposes of identity proofing and/or AB authorization.

- **Identity Proofing**: Consumers may be identity proofed using either the CMS-provided Experian Remote Identity Proofing (RIDP) Risk Based Alternative (RBA) Hub service, or a CMS approved third-party ID proofing service that is compliant with NIST 800-63-4 standards at IAL2 on the respective EDE platform. Consumers who fail identity proofing may be directed to contact the Experian help desk, utilize a CMS-approved third-party ID proofing service if available on the EDE partner platform, or utilize HealthCare.gov to submit their application (which includes creating a HealthCare.gov account to upload ID proofing documentation for manual review).
- **AB Authorization**: EDE partners have the option to choose between a one-time passcode, a one-time confirmation link, or other similar lightweight mechanisms to gather AB authorization information from the consumer.

CMS expects EDE partners to initiate communications with consumers to complete ID proofing and/or provide AB authorization whenever required by CMS' risk-based criteria. EDE partners must ensure that the links and/or passcodes sent to the consumer are single use and are set to expire within 15 minutes of being generated. EDE partners must not send more than three notifications within 24 hours for purposes of gathering identity proofing and AB authorization information for a given AB User ID and Application ID combination. In the event of a non-response from the consumer, EDE partner platforms may allow ABs to manually send a second or third notification to the consumer.

Q4: Does the requirement to gather agent/broker authorization replace the requirement for agents/brokers/web brokers to collect consumer consent?
A4: No. ABs will still be required to obtain and document consent from their consumers. ABs must collect and document consumer consent PRIOR to accessing consumer information or searching for the consumer on EDE platforms. Additional details are outlined in regulation at 45 CFR 155.220(j)(2)(iii), which requires specific documentation prior to assisting with or facilitating enrollment through the FFE or assisting the individual in applying for APTC and Cost-Sharing Reductions (CSRs) for Marketplace plans. ABs who are aware of others conducting a search for consumer applications using approved Classic Direct Enrollment (DE)/EDE websites, or enrolling consumers without their documented consent, or otherwise inappropriately accessing CMS systems should report it to the Agent and Broker Email Help Desk at FFMProducerAssisterHelpDesk@cms.hhs.gov.

Q5: How should agents, brokers, and web brokers handle instances where consumer contact information is outdated or incorrect?
A5: For new consumers, ABs must work with their clients to collect a phone number and an email address that is accessible by the consumer for purposes of identity proofing and AB authorization. There are a few options for returning consumers who have incorrect/outdated information:

- Consumers on the FFE may reach out to the Marketplace Call Center to update their contact information. Consumers will make this update themselves (that is, without the AB on the line). Please see Question 11 for more information.
- Consumers may submit an application through a consumer pathway (via HealthCare.gov or through an approved EDE consumer pathway) with their correct contact information.

As a reminder, ABs must never enter their own professional, personal, or company email/phone number or mailing address on a consumer's application. ABs must not create or use dummy addresses or phone numbers in place of the consumer's email/phone number or mailing address. The consumer or the consumer's authorized representative, and not the AB, must be able to directly access the email account or phone number entered on the application.

Q6: How should ABs handle scenarios where the consumer fails identity proofing?
A6: Generally, consumers who are unable to pass identity proofing through the Experian RIDP RBA service are required to reach out to the Experian telephone help desk. EDE partner platforms must appropriately guide the consumer by providing the consumer with a reference number and contact information for the Experian help desk. In the event that the consumer is unable to verify their identity through the Experian help desk, some EDE partners with CMS approved third-party ID proofing services may use those services to identity proof the consumer. ABs will be blocked from proceeding through the application and/or enrollment process until identity proofing and AB authorization are completed. EDE partner platform UIs must include front-end messaging that indicates if/when an AB can proceed.

Q7: How long are consumer ID proofing and AB authorization valid for?
A7: The foundational goal of identity proofing and AB authorization is to ensure that the consumer is who they say they are, to ensure that the consumer is in control of who is acting on their behalf, and to protect consumers from bad actors.

- Consumer ID proofing may remain evergreen on a given EDE platform if a consumer has an account on that EDE platform and their ID proofing credentials are tied to it. In the absence of a consumer account, consumer ID proofing must be reconfirmed for each coverage year.
- AB authorizations should be gathered every plan year, including for consumers who have existing consumer accounts on a given EDE platform. When a consumer authorizes an

AB, that authorization lasts for the plan year until the consumer authorizes a different/new AB.

Q8: Are agents/brokers/web brokers allowed to complete ID proofing and collect authorization from existing consumers in advance of the Open Enrollment for 2027?
A8: CMS anticipates that ABs may be able to proactively identity proof consumers ahead of Open Enrollment 2027 based on EDE partner implementation. For example, ABs may work with their consumers to proactively complete account creation and ID proofing so that they can be stored as evergreen on a given EDE platform. However, because AB authorizations are applicable to an application for a given plan year, the majority of consumers will likely need to re-authorize their existing AB during Open Enrollment for 2027.[6]

Q9: Is AB authorization required to upload documents on behalf of the consumer to resolve any open Data Matching Issues (DMIs) or Special Enrollment Period (SEP) Verification Issues (SVIs)?
A9: Yes. ABs who upload documents on behalf of the consumer to resolve any open Data Matching Issues (DMIs) or Special Enrollment Period (SEP) Verification Issues (SVIs) request AB authorization if they aren't already authorized by the consumer. Only a single AB user ID may be associated with an application ID at a time.

Q10: To what extent does this impact the InvalidAction error implemented on July 19, 2024, that prevents a new agent from making changes to a consumer's existing FFE enrollment without a three-way call?
A10: For Open Enrollment 2027, CMS will sunset the InvalidAction error and direct EDE partners to sunset any previously approved "pathway switch" functionality on EDE platforms.

On July 19, 2024, CMS implemented program integrity changes to block an AB from making changes to a consumer's FFE enrollment unless the AB is already associated with the consumer's enrollment. If an AB that is new or unassociated with the consumer's existing enrollment attempts to make changes to a consumer's enrollment, the EDE partner platforms receive an InvalidAction error and direct the AB to take additional steps (such as a three-way call with the Marketplace Call Center) to update the consumer's enrollment. With the implementation of new identity proofing and AB authorization requirements on the EDE A/B pathway, this system block is no longer required. CMS will issue additional information in the coming months regarding this change. CMS will continue to monitor any malicious or inappropriate activity by ABs on the Marketplace and will take additional appropriate action against ABs engaged in misconduct.

Q11: Is CMS considering any changes to the Marketplace Call Center?

[6] EDE partners have the option of 'grandfathering in' ABs who are already associated with a given consumer's application once these changes are implemented.

A11: One of the Marketplace Call Center's top priorities is keeping consumers' health care coverage and personal information safe. For Open Enrollment 2027 and beyond, the Marketplace Call Center will no longer support changes to or submission of applications or enrollments that are requested by an AB. This is because the implementation of this new EDE Change Request will newly allow ABs to submit applications and enrollments after the consumer is identity proofed and the agent or broker is authorized to act on the consumer's behalf. In other words, ABs can utilize the EDE A/B pathway to complete activities that previously required a three-way call (such as plan switches).