Best Practice: Ceding Policy Data Client Authorization and Access

Purpose and Scope

This Best Practice provides guidance for obtaining and managing client authorization for the release of ceding policy data during an annuity replacement. This authorization framework was developed with input from legal and compliance professionals within various IRI insurance company member firms.

The authorization process applies when a financial professional is completing a new annuity application, through electronic order entry involving a replacement and requesting information about an existing contract for which they are not currently listed as the financial professional and broker-dealer of record. This Best Practice does not apply in situations where the requesting financial professional and broker-dealer is already associated with the existing contract.

In these situations, the requesting financial professional or distributor must obtain authorization from the client before contract information is approved for release by the ceding carrier or a solution provider on their behalf. This authorization supports the secure exchange of contract data needed to evaluate, process, and support replacement transactions while maintaining appropriate client privacy, consent, and access controls. Without a consistent authorization framework:

- Carriers and distributors may apply different authorization, validation, retention, and access practices, creating friction, rework, and inconsistent client experiences.
- Clients may be required to repeatedly provide duplicative authorization for related servicing or replacement evaluation activities.
- Firms may lack consistent guidance for reusable authorization, custodial account validation, restricted contracts, and audit visibility.
- Participants may over-share sensitive restricted details, apply inconsistent access controls, or under-document authorization evidence, increasing legal, privacy, operational, and client-protection risk.
- Variations in authorization structure may limit interoperability, increase implementation complexity, and slow adoption.

Recommended Best Practices

Authorization Framework

- Firms should support a standardized authorization data model and model consent language that establishes minimum required authorization elements while allowing firms flexibility in legal formatting and presentation.
- Authorization should support digital-first and API-enabled workflows, including e-signature and auditable electronic consent capture.
- Minimum Required Authorization Elements:
    - the contract owner(s) or authorized party(ies), including individual owners, joint owners, trusts, corporate-owned contracts, and other applicable ownership structures,
    - applicable contract(s),
    - the requesting distributor and financial professional,
    - the purpose of the request,
    - and the duration and scope of consent.
- Authorization should support reusable consent for activities directly related to the evaluation and execution of the replacement transaction, such as obtaining updated contract information, conducting replacement analysis, and fulfilling replacement-related requirements, for a defined duration while allowing revocation by the client at any time.
- Firms may continue to apply additional legal, privacy, compliance, or contractual requirements consistent with their internal policies.

Access and Identity Controls

- Authorization and access should be associated with the individual financial professional and authorized support staff, while allowing supervision and governance at the firm level.
- Firms should maintain auditable records of authorization capture, access requests, and data usage consistent with their records obligations.
- Ceding carriers should have access to audit visibility or reporting regarding requests made against their contracts, without requiring manual approval or workflow intervention for each request.

Restricted Contracts and Privacy Controls

- Firms should maintain the ability to restrict access to contract data for fraud, elder abuse, litigation, law enforcement, regulatory, privacy, contractual, or other client-protection concerns.
- When access is restricted, firms should avoid exposing sensitive restriction details and instead use generalized restriction indicators or controlled-access messaging where appropriate.
- Restriction handling processes should support operational consistency while minimizing unnecessary disclosure of sensitive information.

Recommended Authorization Release

Below is a suggested consent form that allows a contract owner to authorize a ceding carrier (or its solution provider) to release their existing annuity contract information to a distributor and financial professional. It's used when a financial professional evaluating or processing a potential 1035 exchange isn't already the financial professional or broker-dealer of record on that contract, and needs documented client consent before the ceding carrier will release the data.

Contract Owner's Authorization to Release Ceding Policy Data

I/We, the undersigned Contract Owner(s) or authorized party(ies), authorize [Ceding Carrier/Solution Provider] to release information regarding the annuity contract(s) identified below to [Distributor] and [Financial Professional, for purposes of evaluating and processing a potential annuity replacement.

Contract Number(s): _____
Ceding Carrier: _____

This authorization permits the release of contract information reasonably necessary to evaluate the existing contract, complete replacement-related requirements, and support the evaluation and execution of the proposed replacement transaction. This authorization is valid through [expiration date / period] and may be revoked at any time by the Contract Owner(s), subject to applicable law and firm requirements.

This authorization may be completed and signed electronically where permitted by applicable law.

Contract Owner / Authorized Party Name: _____
Signature: _____Date: _____
Additional Contract Owner / Authorized Party Name: _____
Signature: _____Date: _____

Out of Scope

This Best Practice does not:

- address whether a proposed replacement is permissible, appropriate, or otherwise valid under applicable legal, regulatory, contractual, product, or firm-specific requirements,
- require firms to use identical legal forms or wording,
- eliminate firm-specific legal or privacy requirements,
- require unrestricted access to contract data,
- or prohibit firms from applying additional fraud, compliance, supervisory, contractual, or client-protection controls.