NGX-F215343: Rx Enabler (Arch) – Correct RX Access for Carved-out Members

# Feature Summary

Objective: Prevent display or use of pharmacy claims and prescriptions that fall outside a member’s Aetna-covered period when the member’s pharmacy history originates from CVS Caremark. CVS systems legitimately maintain a longitudinal (lifetime) prescription history for an individual, spanning time periods when the person may have had other insurers or no coverage at Aetna. When Aetna consumes CVS data via the Consolidated Claims and related APIs, those lifetime records can include fills that pre‑date (and in some cases post‑date) the member’s Aetna plan effective dates. If unfiltered, these records would be visible in Aetna Health and could be acted upon by downstream services.

Solution: Introduce a Policy Effective Window Filter that gates visibility and use of any CVS‑sourced prescription claim, order, or refill. The filter constrains records to the intersection of: (a) the member’s pharmacy membership effective window that aligns with the Aetna plan effective dates, (b) the client’s requested startDate/endDate, and (c) attestation‑controlled integration state. Only claims with fillDate within this window are eligible for display and subsequent flows (detail, order, refill). The integration itself is governed by the ‘CVSRxCarveOut’ feature toggle/attestation; when enabled, Aetna presents embedded capabilities and SSO; when disabled, Aetna presents a limited, link‑out experience.

# Discovery

End‑to‑end prescription management touches multiple services and rules. The discovery synthesized the following dependencies, implications, and constraints that must be addressed uniformly to avoid inconsistent behavior:

1) Data & Authorization Dependencies:  
 • CVS Auth (patient profile) issues a token used by Aetna to call CVS backends.  
 • Consolidated Claims (/getClaimsHistory) returns all visible plan‑member claims for the authenticated member.  
 • Core Proxy (/userauthorizations) and Member Profile (/familyaccessrules) supply authorization and dependent visibility.  
 • UAF privacy checks further restrict access (e.g., HIPAA privacy restrictions, sensitive medications).

2) Filtering & Normalization Dependencies:  
 • Policy Effective Window Filter uses pharmacy membership effectiveStart/effectiveEnd to bound results.  
 • Request window validation requires startDate and endDate; errors if missing.  
 • Deduplicate by uniqueRxId and retain the latest fillDate for list responses.  
 • Final restriction by membershipResourceIds if provided.

3) Integration Surface Area:  
 • Five key integrations (PLP, PDB, PlaceOrder, Ship Consent, i90) depend on consistent claim visibility.  
 • ~47 related APIs rely on the same underlying data and rules; front‑end logic cannot diverge.  
 • A crosswalk/mapping layer is required to align identifiers and payloads across systems.

4) Behavioral Edge Cases to Handle:  
 • Claims with fillDate before plan effectiveStart: exclude.  
 • Orders/refills that straddle coverage boundaries: exclude or block action if outside window.  
 • RefillsLeft = 0 or missing: ensure accurate messaging and no spurious eligibility.  
 • Attestation off (no integrated carve‑out): present limited, link‑out experience.  
 • Missing dates or invalid ranges: return 400 with actionable error details.

5) Caching, Observability, and Security:  
 • Cache key includes account idSource~idValue, membershipResourceId, startDate, endDate.  
 • Log decision points (authorization, privacy, effective window trimming, dedup) for auditability.  
 • Enforce HIPAA and PHI handling standards; secure token exchange and storage.

# Options

## Option 1: Centralized Eligibility & Display Logic Service

Centralize claim visibility rules in a middleware service that evaluates attestation flags, plan effective dates, and carve‑out status before returning data to clients. This ensures consistency across all integrations (PLP, PDB, PlaceOrder, Ship Consent, i90) and eliminates undocumented front‑end logic.

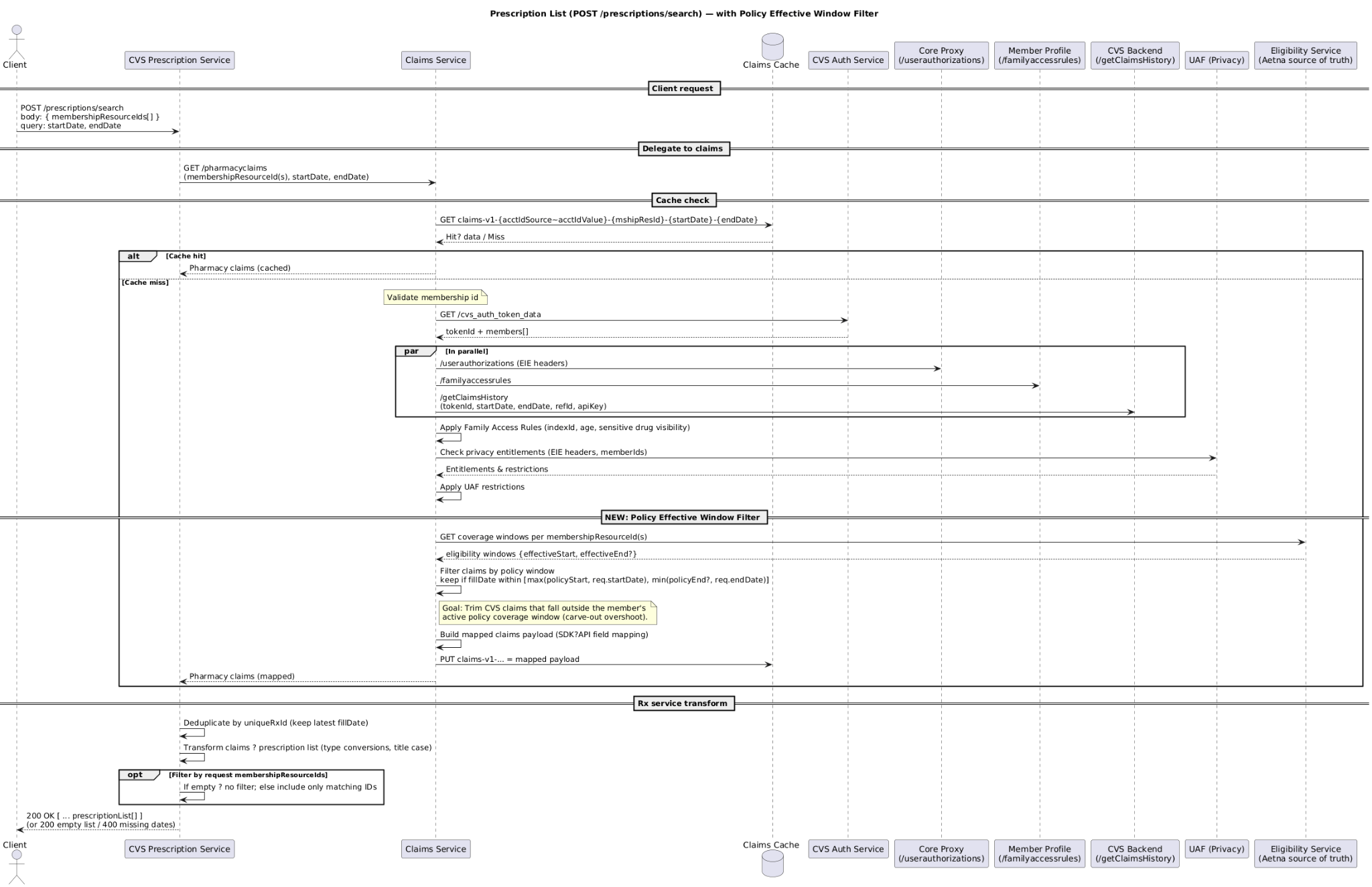
## Option 2: Distributed Logic in Clients

Embed a shared validation library in each integration to enforce claim visibility rules locally. This offers independence but risks divergence over time.

Selected: Option 1 – Centralized service approach for scalability and compliance.

# Solution Sketch

The following diagram illustrates the updated Prescription List Flow with Effective Date Policy Filtering applied. It replaces the previous orchestration placeholder and demonstrates where effective date filtering is enforced.



# Service Logic

The centralized eligibility service enforces claim visibility rules in this order:  
1) Validate attestation (CVSRxCarveOut) and integration state.  
2) Retrieve CVS token (patient profile), authorizations, family access rules, and privacy entitlements.  
3) Fetch claims and normalize; deduplicate by uniqueRxId keeping the latest fillDate.  
4) Apply Policy Effective Window Filter using pharmacy membership effective dates ∩ request window.  
5) Apply family access/UAF privacy restrictions.  
6) Restrict by membershipResourceIds if provided and return mapped responses.

# Services

• CVS Auth Service (patient profile token)  
• CVS Consolidated Claims Service  
• Prescription List Service (POST /prescriptions/search; GET /prescriptions/detail)  
• Order & Refill Service  
• Core Proxy (/userauthorizations)  
• Member Profile (/familyaccessrules)  
• UAF (privacy)  
• **Centralized Eligibility Middleware (Effective Date & Attestation Filtering)**

# Non-Functional Requirements (NFR)

Performance: Response ≤ 200ms under normal load.  
Scalability: Support ~47 APIs and five key integrations.  
Caching: Use deterministic cache keys and TTL aligned with CVS freshness.  
Observability: Emit metrics and traces for cache hits, trims by window, privacy filters, and dedup.  
Reliability: Graceful degradation when dependencies are unavailable.

# Scenarios

1) Prescription claim before coverage effectiveStart → excluded from all views and actions.  
2) Refill/order outside coverage window → blocked with clear messaging.  
3) Member without signed attestation → link‑out (no embedded capabilities).  
4) Member with signed attestation → full embedded integration.  
5) Missing startDate/endDate → 400 Bad Request with guidance.  
6) Sensitive drug + privacy restriction → excluded per UAF.

# Security Review

• All calls use TLS; tokens stored and rotated per policy.  
• PHI/PII minimized, masked in logs; privacy decisions audited.  
• Access governed by EIE headers, family access, and UAF entitlements.  
• Regular reviews with Security for control effectiveness.

# Client Changes

• Integrate with centralized eligibility service for consistent filtering.  
• Enforce and display messaging when items are hidden due to effective dates or privacy.  
• Respect attestation state to show embedded features vs link‑out.  
• Keep UI and mobile parity across platforms.