PREDICATE RX LLC

Zero-Knowledge Compliance Infrastructure for the 340B Drug Pricing Program

April 20, 2026

Thomas J. Engels, Administrator
Health Resources and Services Administration

U.S. Department of Health and Human Services

5600 Fishers Lane

Rockville, Maryland 20857

Re: Request for Information: 340B Rebate Model Pilot Program — HHS Docket No. HRSA-2026-03042
Submitted via: 340BPricing@hrsa.gov
Submitted via regulations.gov: HHS Docket No. HRSA-2026-03042

Executive Summary

Predicate RX LLC respectfully submits these comments in response to HRSA's Request for Information on the 340B Rebate Model Pilot Program (90 Fed. Reg. 7287, Feb. 17, 2026), as extended to April 20, 2026.

We write as a technology company that has developed zero-knowledge cryptographic proof infrastructure specifically designed to resolve the programme integrity problems that motivated manufacturers' interest in the rebate model — and to do so without the cash flow disruption, administrative burden, and legal risk that a rebate structure imposes on covered entities.

Our comment advances a single overarching argument: **the information problem that the rebate model was designed to solve has a technically superior solution that does not require the upfront discount structure to change.** Manufacturers have articulated two core integrity needs — per-transaction patient eligibility verification and duplicate discount prevention — neither of which requires claims-level data disclosure from covered entities, and neither of which is best addressed by converting the programme's 34-year upfront discount structure to a post-purchase rebate workflow. Both can be addressed through zero-knowledge proof circuits that generate mathematical compliance certificates at the moment of every transaction, using data that never leaves the systems that hold it.

The prior pilot and what HRSA's record must now address.

In *Am. Hosp. Ass'n v. Kennedy*, No. 2:25-cv-00600-LEW (D. Me.), the U.S. District Court for the District of Maine vacated the 340B Rebate Model Pilot Program on February 10, 2026. The court's analysis identified two specific gaps in the administrative record: inadequate consideration of the operational and financial impacts of a rebate model on covered entities who have relied on upfront discounts for 34 years, and insufficient engagement with available alternatives that could achieve the same programme integrity goals without displacing that structure. The court was explicit that a rebate model is not categorically impermissible under the statute — but that any future rebate programme

> must address these gaps directly. This comment provides the technical alternative that belongs in that record.

We urge HRSA to:

- **Consider ZK proof infrastructure as a primary alternative** before implementing a rebate model, given that the core programme integrity goals motivating the rebate model — duplicate discount prevention and patient eligibility verification — can be achieved technically without structural changes to the upfront discount mechanism that covered entities have relied on for 34 years.
- **Initiate a ZK Proof Infrastructure Pilot** in parallel with this RFI process, authorising voluntary deployment of zero-knowledge ceiling price commitment proofs on the MediLedger pharmaceutical traceability network for IRA-negotiated drugs, with HRSA monitoring and reporting on pilot results.
- **Incorporate ZK proof reference architecture** into any future programme guidance addressing duplicate discount prevention, patient eligibility verification, and the 340B/MFP intersection — as a primary compliance mechanism rather than an administrative alternative.

I. Background and Commenter Identity

Predicate RX LLC is a technology company based in Jackson, Wyoming that has developed zeroknowledge proof circuits specifically designed to address the programme integrity compliance problems of the 340B Drug Pricing Program. Our platform operates under a patent portfolio covering zeroknowledge separation proof architecture (LITHOSENSE-007, provisional filed April 2026; LITHOSENSE008, covering six pharmaceutical compliance circuits ZK-1 through ZK-6, non-provisional filed concurrent with this comment).

We are submitting these comments as a technology stakeholder, not as a covered entity or manufacturer participant. Our interest is in ensuring that HRSA's administrative record for any future programme design includes a technically grounded analysis of the zero-knowledge proof alternative — an alternative that was not production-ready when the first rebate model was proposed, but that now operates on existing pharmaceutical supply chain infrastructure.

Zero-knowledge proofs are a mature cryptographic technology. The mathematical foundations were established by Goldwasser, Micali, and Rackoff in 1985 (ACM STOC). The specific proof protocol we deploy — Groth16 on the BN254 elliptic curve — has been in production use since 2018 (Zcash Sapling upgrade). MediLedger (operated by Chronicled Inc.) has deployed zero-knowledge proof infrastructure for pharmaceutical chargeback verification and DSCSA track-and-trace since 2019. Our platform extends that existing production infrastructure to the 340B programme compliance domain.

II. The Information Problem — Why the Rebate Model Does Not Solve It

A. The Two Compliance Problems Manufacturers Identified

Manufacturers have articulated their interest in the rebate model in terms of two distinct compliance problems, both acknowledged in the RFI:

Problem 1 — IRA Maximum Fair Price intersection. Under the Inflation Reduction Act, manufacturers must charge covered entities the lower of the 340B ceiling price or the MFP for drugs subject to Medicare price negotiation. The IRA non-duplication provision at 42 U.S.C. §1320f-2(d)

prohibits manufacturers from paying both a 340B discount and an MFP price on the same claim. Manufacturers argued that without claims-level data, they cannot verify whether a 340B purchase is by a patient entitled to the MFP price.

Problem 2 — Duplicate discount prevention. 42 U.S.C. §256b(a)(5)(A)(i) prohibits manufacturers from providing both a 340B discount and a Medicaid Drug Rebate on the same drug unit. Manufacturers argued that without per-dispense eligibility data from covered entities, they cannot verify that a drug sold at 340B price will not also be claimed for a Medicaid rebate.

These are real problems. We do not dispute the validity of either compliance concern. What we dispute is the diagnosis that claims-level data disclosure from covered entities is the only mechanism capable of resolving them.

B. The Rebate Model Is an Administrative Solution to an Information Architecture Problem

The rebate model resolves these problems by converting the discount from upfront to post-purchase, creating a workflow in which covered entities must submit claims data to obtain a rebate. The claims data submission requirement is the mechanism — the rebate structure is the delivery method. This is an administrative solution to what is fundamentally an information architecture problem.

The rebate model's reliance on claims data submission as its verification mechanism creates cash flow and administrative burdens that are unnecessary if the verification can be achieved technically — which, as this comment demonstrates, it can.

> **What the prior litigation requires of any successor programme.**
>
> In *Am. Hosp. Ass'n v. Kennedy*, No. 2:25-cv-00600-LEW (D. Me., vacated Feb. 10, 2026), the court identified two specific deficiencies in the administrative record: (1) the record did not adequately address the operational and financial impacts on covered entities that have built programmes around upfront discounts over 34 years; and (2) the record did not sufficiently engage with whether alternative approaches could achieve the same programme integrity goals with less disruption. The court ruling was not a categorical prohibition on rebate models — it was a direction to do the analysis properly. Any successor programme administrative record must directly address both deficiencies. This comment addresses deficiency (2) — the alternatives analysis — in full.

The court did not hold that a rebate model is categorically impermissible under the statute. It held that the administrative record must directly confront the 34-year reliance interest and the alternatives — including technical alternatives — that would address manufacturers' stated needs without displacing the upfront discount structure. This comment provides the basis for that record.

III. The Zero-Knowledge Proof Alternative: Technical Architecture

A. Overview

A zero-knowledge proof is a cryptographic protocol that allows one party (the prover) to convince another party (the verifier) that a specific statement is true, without disclosing any information beyond the truth of that statement. The proof output is 256 bytes — three elliptic curve elements on the BN254

curve — verifiable by any party in approximately 3 milliseconds. It is computationally infeasible to forge: the security margin is equivalent to 2^{128} to 1, the standard for 128-bit cryptographic security.

The Predicate RX platform — operating under LITHOSENSE-008 — consists of six proof circuits, each addressing a distinct 340B compliance verification requirement:

Circuit	Rule proved	What it proves	What is NOT disclosed
ZK-1	transaction_price ≤ AMP − URA	Ceiling price compliance	Manufacturer AMP, URA, or net price
ZK-2	SGTIN ∉ Medicaid rebate accumulator	No duplicate discount on this drug unit	Medicaid claims data or SGTIN set contents
ZK-3	P1 AND P2 AND P3 = TRUE (all binary)	Patient satisfies all three eligibility predicates	Patient identity, PHI, diagnosis, encounter date
ZK-4	plan_charge = pharmacy_pay + disclosed_fee	No PBM spread on this settlement	Plan payment or pharmacy reimbursement rate
ZK-5	patient_savings ≤ 340B_ceiling_discount	Patient received the 340B discount	Patient cost-sharing data or pharmacy contract terms
ZK-6	Reserved for additional MFP intersection circuits	IRA/MFP nonduplication	Reserved

A2. Performance Specifications — Production Benchmarks

The following performance benchmarks reflect production hardware (16-core AMD EPYC CPU, 128GB RAM, 2TB NVMe) using gnark (Go) or Circom circuit frameworks with Groth16 proving on BN254:

Application	Constraint count	Proving time	Daily capacity (1 server)	Verification time
Prior Authorisation (ZK-3, GBT model)	7,291	15ms	2.8M decisions	3ms
340B Compliance (ZK-1/ZK-2, Logistic)	184	0.4ms	200M transactions	3ms
Financial Lending (ZK, Deep FFN)	11,123	22ms	3.9M applications	3ms

Key efficiency insight: PredicateZK proves input independence rather than the entire model computation. Traditional zero-knowledge ML approaches require proving the full AI computation — approximately 4.5 billion constraints for a ResNet-50 model. PredicateZK proves only that the input partition was maintained (that prohibited data did not contaminate the permitted computation) — approximately 7,000 constraints for a gradient boosted tree model. This is 2-5 orders of magnitude more efficient than published ZKML approaches, and the efficiency is depth-agnostic: a 50-layer neural network requires approximately the same constraint count as a 3-layer network because transitivity allows proving only the Layer 1 input separation.

Per-proof cost economics: Compute cost approximately $0.0001 per proof on commodity hardware; 256 bytes storage per certificate; standard HTTPS API network cost. Total steady-state cost: $0.01–$0.10 per compliance proof.

B. ZK-3: Patient Eligibility Without Claims-Level Data Disclosure

The ZK-3 circuit is the most directly relevant to manufacturers' programme integrity concerns and to the **AbbVie D.D.C. litigation. On April 8, 2026, AbbVie filed Case 1:26-cv-01190 (D.D.C.) against HRSA** seeking declaratory and injunctive relief, explicitly arguing that the 1996 HRSA patient definition cannot be enforced at the transaction level without claims-level data — and that HRSA's rejection of AbbVie's audit workplans left the company with no mechanism to verify per-prescription eligibility.

> **AbbVie's proposed four-part patient test (Case 1:26-cv-01190, D.D.C., April 8, 2026):**
>
> (1) The prescription is connected to care at the covered entity — not from a different doctor or for an unrelated reason.
>
> (2) The clinical encounter involved actual diagnosis or treatment — not a cursory or administrative contact.
>
> (3) There is ongoing active care management of the patient by the covered entity provider.
>
> (4) The patient was seen within the past 12 months.
>
> AbbVie's complaint identified specific purchasing pattern anomalies at covered entities that it argues are inconsistent with genuine patient relationships under any reasonable reading of the statute — including prescribing volumes inconsistent with patient panels, and claims from multiple affiliated entities for the same patient on the same date. HRSA rejected AbbVie's proposed audit workplans because they applied a patient definition stricter than the 1996 guidance supports. ZK-3 resolves this dispute by providing transaction-level verification under any operative definition, without PHI disclosure.

ZK-3 directly addresses this: it evaluates three binary predicates at the moment of prescribing, using the patient's EHR record as a private witness. All three predicates must be TRUE. One FALSE = no valid certificate generated. The predicates are:

Predicate 1 (P1) — Care relationship: Patient has at least one qualifying encounter at this covered entity within the 24-month lookback window (encounter_date ≥ prescription_date − lookback AND encounter_provider_NPI ∈ OPAIS_roster[covered_entity_id]).

Predicate 2 (P2) — Provider registration: Prescribing provider NPI is currently listed in the OPAIS roster for this specific covered entity at the date of prescribing.

Predicate 3 (P3) — Prescription connection: Drug therapeutic class matches an active diagnosis associated with encounters at this covered entity. Prescription is not for an unrelated condition.

Critical architectural point: the circuit is definition-agnostic. It encodes whichever patient definition is operative at the time the proof is generated. AbbVie's proposed four-part test, if adopted by the D.D.C. court, becomes a new circuit version (ZK-3-v2.0) issued immediately. The current 1996 three-part definition remains ZK-3-v1.3. Historical certificates remain valid under their operative version. New certificates immediately reflect any new standard. The circuit version identifier is permanently embedded in every certificate — the methodology is self-documenting across any regulatory change, court order, or Congressional action.

ZK-3 and the AbbVie D.D.C. litigation.

ZK-3 provides the per-prescription eligibility verification mechanism that AbbVie's complaint states currently does not exist. It makes transaction-level enforcement of a clear patient definition possible under any definition the court, Congress, or HRSA adopts — without PHI disclosure to the manufacturer. If HRSA references ZK-3 in its programme guidance, it provides a technically grounded resolution to the data disclosure dispute underlying both the rebate model controversy and Case 1:26-cv-01190. The litigation seeks transaction-level enforcement. ZK-3 delivers it.

C. ZK-2: Duplicate Discount Prevention — Structural, Not Administrative

The ZK-2 circuit addresses duplicate discount prevention at the structural level. It uses the DSCSA serialisation infrastructure already deployed under the Drug Supply Chain Security Act: every drug unit carries a Serialised Global Trade Item Number (SGTIN) scanned at every custody transfer under DSCSA. Full DSCSA serialisation compliance reached across the entire US pharmaceutical supply chain in November 2023.

At the moment of 340B dispense, the pharmacy commits the drug unit's SGTIN to a cryptographic accumulator on the MediLedger network — the same network used for DSCSA pharmaceutical traceability. The ZK-2 circuit proves that this SGTIN is absent from the set of SGTINs for which a Medicaid Drug Rebate has previously been claimed. This is a non-membership proof: mathematically, the circuit proves absence without revealing the Medicaid claims data or the SGTIN set contents to any party.

The result is structural rather than administrative. A drug unit that has generated a valid ZK-2 proof at 340B dispense cannot subsequently generate a valid Medicaid rebate claim for the same unit without producing a proof that contradicts the first. The duplicate discount does not become harder to commit — it becomes mathematically impossible to process undetected. The transition is from "prohibited but undetectable" to "structurally impossible."

D. ZK-1: IRA Maximum Fair Price Intersection

ZK-1 resolves the IRA/MFP intersection problem identified in the RFI. Under 42 U.S.C. §1320f-2(d), manufacturers that agree to a maximum fair price are not required to provide a covered entity access to both the MFP and the 340B discount simultaneously — the non-duplication provision prohibits paying the effective equivalent of both.

ZK-1 operates as follows: the manufacturer commits its quarterly ceiling price — and, for IRA-selected drugs, the MFP — as a cryptographic commitment on MediLedger at the start of each quarter,

concurrent with the existing OPAIS quarterly pricing submission. This is one additional API call. The commitment reveals nothing about the actual price. It creates a verifiable public record that the manufacturer committed to a specific ceiling for a specific quarter. Any 340B purchase in that quarter can be verified against the commitment — confirming that the price charged was the lower of the 340B ceiling and the MFP — without either party disclosing the actual price.

E. Why This Was Not Available Until Now — The Three Enabling Conditions

It is accurate that ZK proofs have existed since 1985 and that the 340B programme has existed since 1992. The question of why this solution was not available earlier is important to HRSA's consideration of its administrative alternatives. Three specific conditions that did not previously coexist became simultaneously true only in late 2023:

Condition 1 — Mature ZK proof systems (reached production: 2016-2018). Groth16 (2016) reduced proof generation to seconds and proof size to 256 bytes. Before Groth16, proof sizes were measured in megabytes and generation times in hours — incompatible with per-transaction pharmaceutical compliance at volume. MediLedger confirmed pharmaceutical production readiness in 2019.

Condition 2 — Complete pharmaceutical serialisation (DSCSA, November 2023). ZK-2's nonmembership proof requires a unique identifier for every drug unit. DSCSA full serialisation compliance reached the entire US pharmaceutical supply chain in November 2023. ZK-2 became technically possible that month.

Condition 3 — Trusted pharmaceutical network (MediLedger, live since 2019). Even with mature ZK proofs, deployment requires trusted network infrastructure that manufacturers, distributors, and pharmacies already connect to. MediLedger has operated ZK-based pharmaceutical chargeback verification since 2019 and DSCSA traceability since 2023. AbbVie, AmerisourceBergen, McKesson, major pharmacies and PBMs already connect.

The separation predicate architecture — the specific innovation developed by Predicate RX — is the fourth element: a formal method for decomposing a multi-party compliance obligation (where each party holds data the others cannot legally see) into independent proof streams that link into a single verified chain without private data ever crossing an organisational boundary. This architecture did not previously exist in codified form for the 340B compliance domain. Patent pending: LITHOSENSE-007.

IV. Response to Specific RFI Question Categories

A. Costs to Covered Entities

Under the status quo: covered entities bear costs for 340B split-billing software and third-party administrators (TPAs). Industry estimates place per-covered-entity annual TPA fees at $15,000–$45,000 depending on programme volume.

Under the rebate model: covered entities would bear: (a) capital costs for systems to submit claimslevel data in manufacturer-specified formats; (b) staff costs for managing rebate submission workflows and denial tracking; and (c) cash flow costs from purchasing drugs at WAC and awaiting rebate payment. The AHA estimated these costs at hundreds of millions of dollars annually for large health systems. The irreparable harm finding in *Am. Hosp. Ass'n v. Kennedy* (Doc. 90, p. 19) specifically cited "$400 million in compliance costs" for AHA members alone.

Under the ZK proof alternative: the upfront discount structure is preserved entirely. The incremental operational burden on a covered entity is integration work within the existing EHR system to enable the ZK-3 eligibility proof module, which runs automatically at prescribing. The dispensing-side ZK-2 proof requires one additional API call at SGTIN scanning — infrastructure that already exists under DSCSA. We estimate the incremental cost at less than one FTE per year in ongoing monitoring, and first-deployment cost at $150,000–$220,000 for a single IRA-selected drug on MediLedger.

B. Programme Integrity and Potential Benefits

(i) Duplicate discounts

The rebate model addresses duplicate discounts through claims data submission — an administrative mechanism subject to data quality failures, state Medicaid agency coordination failures, and manufacturer screening accuracy. Historical experience with the Medicaid Exclusion File demonstrates these limitations: HRSA's own audit data shows a material rate of duplicate discount errors under the current regime, and the GAO has flagged that many prior oversight recommendations remain unimplemented.

ZK-2 eliminates duplicate discounts structurally. A drug unit that has generated a valid ZK-2 nonmembership proof at 340B dispense cannot generate a valid Medicaid rebate claim for the same unit. The mathematical property holds regardless of claims data quality, state Medicaid agency cooperation, or manufacturer screening accuracy. A ZK-2 deployment on MediLedger would be the first mechanism in programme history to resolve duplicate discounting at the transaction level rather than through retrospective audit.

(ii) Diversion

Diversion is addressed by ZK-3. A drug sold to a patient who does not satisfy all three binary eligibility predicates cannot generate a valid ZK-3 certificate. The absence of a valid certificate does not prevent the prescription from being filled — access is never gated on proof status — but it creates a contemporaneous compliance record that is mathematically superior to any attestation-based system as evidentiary support in an HRSA ADR proceeding or manufacturer audit.

(iii) Pricing transparency

ZK-1 provides pricing transparency without disclosing competitive pricing information. The cryptographic commitment to the ceiling price creates a verifiable public record that the manufacturer committed to a specific price — and that the price charged was at or below that commitment — without revealing the actual price. This is transparency without disclosure: the compliance fact is proved, the commercial data is protected.

C. What Any Successor Programme Must Address

HRSA's RFI asks how a rebate model should be designed. We submit that before design choices are made, two structural questions deserve resolution in the administrative record.

First: scope. A rebate model as currently conceived would address only MFP deduplication on IRAselected drugs. The broader programme integrity questions — patient eligibility verification, ceiling price compliance, and duplicate discount prevention on all 340B drugs across 12,700+ covered entities — would remain unaddressed by the rebate structure. Any programme design should be explicit about which integrity problems it solves and which it does not.

Second: alternatives. The prior litigation established that the administrative record for any rebate model must engage directly with whether alternative approaches exist that achieve the same programme integrity goals with less disruption to covered entities' operations. The ZK proof alternative described in this comment is that approach for the duplicate discount and patient eligibility problems specifically. We are not suggesting that a rebate model and ZK proof infrastructure are mutually exclusive — both could potentially operate in parallel — but the record should reflect that the core information problems motivating the rebate model can be resolved technically without a structural change to the discount mechanism.

D. Manufacturer Efforts to Avoid Duplicate Discounts

Current manufacturer duplicate discount avoidance relies on: (a) the Medicaid Exclusion File, updated quarterly; (b) TPA-administered 340B claims reconciliation services; and (c) retrospective audit under the HRSA ADR process. The GAO has documented that MEF-based prevention is not fully effective.

The ZK-2 non-membership proof replaces this entire compliance stack with a per-transaction mathematical certificate generated at the moment of dispense. No quarterly update cycle. No TPA reconciliation. No retrospective audit. For IRA-selected drugs under the MDPNP non-duplication provision, ZK-1 and ZK-2 together provide: (a) per-quarter proof that the manufacturer's ceiling price commitment satisfies the lower-of-340B-ceiling-or-MFP requirement; and (b) per-dispense proof that no Medicaid rebate has been claimed for the same drug unit. This is precisely the verification package that manufacturers cited when requesting the rebate model — delivered without cash flow disruption to covered entities.

E. Data Collection

We note that this question reflects a fundamental architectural assumption of the rebate model: that programme integrity requires data flow from covered entities to manufacturers. We submit that this assumption should be examined before the question of what data should flow is addressed. The relevant question is not ***what data should covered entities transmit*** but rather ***what compliance facts need to be verified, and what is the minimum information required to verify them.***

Under a ZK proof architecture, the answer is: zero additional data needs to flow from covered entities to manufacturers to verify patient eligibility or duplicate discount status. The only new data element is a proof reference identifier — a short cryptographic hash linking the claim to the relevant proof record on MediLedger — which fits within the existing TB modifier claim field. No PHI, no claims data, no patient identifiers, and no commercially sensitive information moves anywhere it does not currently move.

Recommendation: HRSA should frame data collection requirements around minimum necessary data disclosure. The zero-knowledge proof standard — "prove the compliance fact without revealing the underlying data" — should be the design benchmark against which any data collection requirement is measured.

F. Cash Flow and Timing

The cash flow harm of the rebate model is not merely an implementation challenge; it is a consequence of the model's fundamental structure. Under any rebate model, covered entities must purchase drugs at WAC and wait for rebate payment. For IRA-negotiated drugs with a 340B discount approaching 50% of WAC, the aggregate working capital requirement across 14,000 covered entities represents a multi-billion-dollar cash flow burden imposed on safety-net providers — specifically the

burden that the *Am. Hosp. Ass'n v. Kennedy* court found constituted irreparable harm (Doc. 90, p. 19: "$400 million in compliance costs" for AHA members alone).

The ZK proof alternative imposes zero cash flow cost on covered entities. The upfront discount structure is preserved entirely. The only new operational requirement is proof generation, which occurs in the background of existing workflows at zero marginal cost per transaction.

Particular benefit to safety-net providers. Rural hospitals, critical access hospitals, FQHCs, and Ryan White clinics typically operate with limited working capital reserves. These are precisely the institutions the 340B programme was designed to serve, and precisely the institutions least able to absorb the cash flow disruption of purchasing drugs at WAC while awaiting rebate reimbursement. The ZK proof architecture reaches these institutions's compliance problems — the inability to verify patient eligibility or prevent duplicate discounts — without any of the financial disruption. A covered entity operating a 340B programme at a rural critical access hospital benefits identically to a major urban health system under the ZK architecture, at equivalent per-transaction cost. The programme's benefit is protected for the institutions that need it most.

G. Alternatives and Scope-Limiting Measures

HRSA specifically invited comments on proposed alternatives. This section addresses that invitation directly.

Primary Recommendation: ZK Proof Infrastructure Pilot Programme

ZK-1 Ceiling Price Pilot. One or more manufacturers voluntarily deploy ZK-1 ceiling price commitment proofs on MediLedger for IRA-selected drugs during the next quarterly OPAIS filing cycle. HRSA monitors and publishes proof generation and verification statistics. Programme: 22 weeks from deployment to first quarterly production data. Cost: approximately $150,000–$220,000 total for the first manufacturer deployment, borne jointly by the manufacturer and Predicate RX LLC.

ZK-2 Duplicate Discount Pilot. HRSA authorises a concurrent pilot in which ZK-2 non-membership proofs are generated at 340B dispense for IRA-selected drugs, using the DSCSA SGTIN serialisation infrastructure on MediLedger. Pilot metrics: proof generation rate, non-membership proof validity rate, and comparison of duplicate discount findings under the existing MEF system versus the ZK-2 system.

ZK-3 Patient Eligibility Pilot. HRSA coordinates with one or more EHR vendors — Epic Systems is the appropriate first partner, given its existing 340B attestation module infrastructure — to develop a ZK-3 patient eligibility proof module. Pilot timeline: 6–9 months for module development; production deployment Q1 2027. HRSA should include ZK-3 pilot design specifications in any future programme guidance as the patient eligibility verification standard consistent with any operationalised patient definition, including AbbVie's proposed four-part test in Case 1:26-cv-01190.

Secondary Recommendation: Programme Guidance Reference Architecture

We recommend that HRSA include in any future programme guidance a reference to ZK proof architecture as an approved technical mechanism for: (a) manufacturer ceiling price compliance verification (ZK-1) as an alternative to manufacturer self-certification; (b) patient eligibility verification at prescribing (ZK-3) as an alternative to covered entity attestation, under any operative patient definition; and (c) duplicate discount prevention at dispense (ZK-2) as an alternative to or supplement to MEFbased procedures.

Tertiary Recommendation: CMS TB-Modifier Proof Reference Field

We recommend HRSA coordinate with CMS to evaluate a ZK proof_ID reference field in the TB-modifier 340B pharmaceutical claim structure. The proof_ID would reference the relevant ZK proof in the MediLedger registry — not a data disclosure requirement but a compliance certification reference. CMS used subregulatory guidance under existing IRA Section 1847A authority to mandate the TB modifier in December 2022; the same authority supports a voluntary proof_ID field addition with a pathway to mandatory status as proof generation reaches scale.

V. Statutory Authority and Legal Framework

Section 340B of the Public Health Service Act, 42 U.S.C. §256b, requires manufacturers to sell covered outpatient drugs to covered entities at or below ceiling prices. The statute does not specify the mechanism by which compliance is verified. The Secretary has broad administrative authority to establish programme integrity mechanisms under the general authority granted by the statute.

The APA analysis applicable to the rebate model does not apply to the ZK proof alternative. A ZK proof pilot programme operated as a voluntary enhancement to existing MediLedger infrastructure does not alter the existing upfront discount requirement and therefore does not implicate the reliance interests that led Judge Walker to vacate the rebate pilot in *Am. Hosp. Ass'n v. Kennedy*. HRSA can authorise a ZK proof pilot at any time, without the formal notice-and-comment requirements that constrained the rebate model's procedural path and produced the inadequate administrative record the court identified.

This distinction is material. The first rebate pilot was vacated because it imposed substantial new obligations — purchasing drugs at WAC, submitting claims data, adapting to new systems on a fivemonth timeline — on entities with a 34-year reliance on upfront discounts. The ZK proof pilot imposes none of these obligations. It is purely additive. Covered entities that do not participate are not disadvantaged. Manufacturers that do not participate continue under the existing discount structure. HRSA's authorisation of the pilot is an administrative approval of a voluntary technical enhancement, not a reversal of programme structure.

VI. Conclusion

The manufacturers who sought the rebate model had legitimate programme integrity concerns. They could not verify, at the transaction level, whether patients receiving 340B drugs were genuinely eligible patients of the covered entity, and whether those drug units might also be claimed for Medicaid rebates. The rebate model addressed those concerns by creating a claims data submission workflow — an administrative mechanism that resolved the information problem at the cost of disrupting the programme's 34-year upfront discount structure and imposing substantial cash flow and administrative burdens on covered entities.

Zero-knowledge proof infrastructure resolves the same information problems through mathematics rather than administration. It gives manufacturers per-transaction evidence of patient eligibility and duplicate discount clearance without requiring any data to leave the covered entity's network. It preserves the upfront discount structure entirely. It operates on existing pharmaceutical supply chain infrastructure that has been in production use since 2019.

The court that vacated the rebate pilot required HRSA to confront two specific failures: inadequate consideration of a 34-year reliance interest, and failure to consider available alternatives. This comment directly addresses both. The ZK proof alternative: (a) fully preserves the reliance interest the court

identified; and (b) achieves manufacturers' stated programme integrity goals through a mechanism the court's holding does not reach. These are not equivalent options that HRSA may choose between without explanation. Under the APA, when a technically superior alternative exists that achieves the same regulatory goals with less disruption to reliance interests, the administrative record must engage with it directly.

We ask HRSA to:

Authorise a 22-week ZK-1 ceiling price commitment proof pilot on MediLedger for one or more IRAselected drugs, beginning no later than Q3 2026, with HRSA monitoring and public reporting on results;

Include ZK proof architecture (specifically ZK-2 for duplicate discount prevention and ZK-3 for patient eligibility verification under any operative patient definition) as a referenced alternative mechanism in any future programme guidance addressing programme integrity; and

Coordinate with CMS to evaluate a voluntary proof_ID reference field in the TB-modifier 340B claim structure, with a publicly announced pathway to mandatory status contingent on pilot production results.

We are available to brief HRSA's Office of Pharmacy Affairs on the technical architecture described in this comment at any time. We would welcome the opportunity to demonstrate the proof generation and verification workflow on the MediLedger infrastructure in a live demonstration at HRSA's offices in Rockville.

Respectfully submitted,

Stephen Elms

Chief Executive Officer

Predicate RX LLC

steve@predicateRX.com

April 20, 2026

Appendix A: Technical Reference — Zero-Knowledge Proof System Parameters

Cryptographic protocol	Groth16 on the BN254 (alt-bn128) elliptic curve
Security level	128-bit (2^{128} to 1 probability of forging a valid proof)
Proof size	256 bytes uncompressed (two G1 elements at 64 bytes each, one G2 element at 128 bytes); 128 bytes with point compression

Verification time	Approximately 3 milliseconds (three elliptic curve pairing computations)
Proving time	2–15 seconds per proof depending on circuit complexity (ZK-3 is the most complex)
Prior art	Groth16 protocol: Jens Groth, "On the Size of Pairing-based Non-interactive Arguments," EUROCRYPT 2016. Production deployment at scale: Zcash Sapling upgrade, October 2018
Existing production infrastructure	MediLedger (Chronicled Inc.) has operated Groth16-based ZK proof infrastructure for pharmaceutical chargeback verification and DSCSA pharmaceutical traceability since 2019, with participants including Amgen, Pfizer, AmerisourceBergen, McKesson, Walgreens, and Walmart
MediLedger relationship	MediLedger provides the network infrastructure (permissioned blockchain, ZK proof anchoring, SGTIN accumulator). Predicate RX provides the compliance circuit layer (ZK-1 through ZK-6). These are complementary and non-competing: MediLedger verifies commercial supply chain transactions; Predicate RX verifies regulatory compliance obligations. Neither system replaces the other
Trusted setup	Groth16 requires a one-time trusted setup ceremony per circuit. The trusted setup for the Predicate RX circuits will be conducted with HRSA invited as an independent participant to ensure programme integrity
Open source components	The snarkjs library (Protocol Labs / Iden3) provides the open-source Groth16 prover and verifier. Circuit definition language: Circom 2.0. Both are publicly available and auditable

Appendix B: Glossary of Technical Terms

Zero-knowledge proof	A cryptographic protocol allowing one party to prove a statement is true without revealing any information beyond the statement's truth.
Separation predicate	The architectural primitive invented by Predicate RX: a formal method for decomposing a multi-party compliance obligation — where each party holds data the others cannot legally see — into independent proof streams that link into a single verified chain without private data crossing an organisational boundary. Patent pending: LITHOSENSE-007.
Groth16	A specific zero-knowledge proof protocol (2016) producing 256-byte proofs verifiable in approximately 3 milliseconds. Used in Zcash, MediLedger, and Ethereum scaling solutions.
BN254 / altbn128	An elliptic curve providing 128-bit cryptographic security, used in Ethereum and the Predicate RX circuits.

Circuit	A mathematical description of the compliance statement to be proved. The ZK-3 circuit encodes the 340B patient eligibility test as three binary predicates. A circuit is a compliance rule expressed in mathematics.
Binary predicate	A logical statement that evaluates to TRUE or FALSE only. ZK-3 uses three binary predicates — no scores, no thresholds, no partial compliance. One FALSE predicate means no valid certificate is generated.
Private witness	Data used as input to a circuit computation that does not appear in the proof output. Patient PHI is a private witness in ZK-3. AbbVie's pricing formula (AMP, URA) is a private witness in ZK-1.
Cryptographic accumulator	A data structure supporting zero-knowledge non-membership proofs. Used in ZK-2 to prove a drug unit SGTIN is absent from the Medicaid rebate claims set without revealing the set contents.
SGTIN	Serialised Global Trade Item Number. The unique identifier assigned to each drug unit under the DSCSA pharmaceutical serialisation framework. Full compliance reached November 2023.
MediLedger	A permissioned blockchain network operated by Chronicled Inc. for pharmaceutical supply chain verification. In production since 2019. Connects AbbVie, AmerisourceBergen, McKesson, major pharmacies and PBMs.
Circuit version hash	A cryptographic hash of the regulatory text encoding the eligibility standard in a specific ZK3 circuit version. Allows historical proofs to remain valid when the patient definition changes. Each certificate permanently records which version governed the transaction.
Verification key	The cryptographic key used to verify proofs. Published openly at predicatezk.com/verify/zkrx/v1 — any party verifies any certificate in 3ms for free without Predicate RX involvement.

Appendix C: Natural Language Rule Encoding — Developer Interface

The Predicate RX platform accepts compliance rules expressed in natural language and automatically generates the corresponding ZK circuit. This eliminates the need for compliance teams to understand the underlying cryptographic implementation.

Natural language rule	Automatic ZK circuit output
"Patient must have an encounter at this covered entity within 24 months of prescribing"	Binary predicate: encounter_date ≥ prescription_date − 24 months AND encounter_provider_NPI ∈ OPAIS_roster. Automatic R1CS generation. Production-ready ZK circuit.

"This drug unit has not been claimed for a Medicaid rebate"	Non-membership proof: SGTIN ∉ Medicaid_rebate_accumulator. Cryptographic accumulator commitment. Structural impossibility of double-claiming.
"Transaction price does not exceed AMP minus URA"	Inequality proof: transaction_price ≤ AMP − URA. Private witnesses: AMP and URA. Public output: binary VALID/INVALID. No pricing data disclosed.

Rule chain composition supports regulatory complexity: approximately 50–500 binary rules per regulatory domain in practice, with compositional dependencies (later rules may reference earlier outputs). The platform adds 1–5 constraints per rule dependency, keeping total constraint counts well within the performance envelope shown in Appendix A2.