The Universal Health Architecture & Exchange Protocol (UHAEP)

Part III: The Legislative Statute

Document Reference: `SB-UHAEP-2026-02-LEG`
Draft Bill: 119th Congress, 2nd Session
Topic: The Universal Health Architecture Act of 2026

A BILL

To mandate the transition of federal and commercial health information systems to a decentralized, event-sourced, and decoupled architecture; to establish the Patient Sovereign Root Node; to require the implementation of legacy database wrappers; to prohibit the blocking of clinical workflows by administrative prior authorization; and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) **Short Title**.—This Act may be cited as the **"Universal Health Architecture Act of 2026"**.
(b) **Table of Contents**.—The table of contents for this Act is as follows:

TITLE I—SOVEREIGN PATIENT DIGITAL IDENTITY

SEC. 101. ESTABLISHMENT OF PATIENT SOVEREIGN ROOT NODE.

(a) **In General**.—The Secretary of Health and Human Services (referred to in this Act as the "Secretary"), in coordination with the National Institute of Standards and Technology (NIST), shall establish a cryptographic decentralized identity framework for the issuance of a unique Decentralized Identifier (DID) to every citizen and legal resident of the United States, to be known as the **Patient Sovereign Root Node**.
(b) **W3C Standard Compliance**.—The Sovereign Root Node shall conform to the World Wide Web Consortium (W3C) Decentralized Identifiers standard.
(c) **Ownership of Data**.—
(1) All clinical, demographic, genomic, and diagnostic data generated by any clinical provider during the care of a patient shall be anchored to the patient's Sovereign Root Node.
(2) The patient shall hold sole intellectual property and cryptographic ownership over all data indexed under their Sovereign Root Node. No hospital system, clinic, health insurer, or government agency may assert proprietary rights or restrict transfer of such data.

SEC. 102. PATIENT DELEGATION AND CONSENT.

(a) **Cryptographic Consent Mandate**.—Access to read or write data to a Sovereign Root Node shall be governed by cryptographically signed consent policies utilizing Verifiable Credentials (VCs).
(b) **Emergency Bypass**.—The Secretary shall define cryptographic protocols for

emergency clinical access, which shall generate a self-auditing, high-priority ledger event documenting the justification for emergency access.

TITLE II—NATIONAL EVENT-SOURCED CLINICAL LEDGER

SEC. 201. IMMUTABLE EVENT-SOURCED CARE ENGINE.

(a) **Requirement for EHR Certification**.—Beginning 24 months after the date of enactment of this Act, the Assistant Secretary for Technology Policy (ASTP) shall not certify any Electronic Health Record (EHR) system that does not record clinical care using an event-sourced, append-only cryptographic ledger.
(b) **Prohibition on Overwrites**.—No clinical information system may utilize a database schema that permits the update, deletion, or overwrite of clinical entries.
(c) **Historical Ledger Record**.—All historical records of care, medication administrations, diagnoses, and measurements shall remain permanently visible and unaltered in the patient's event ledger. Any correction, cancellation, or amendment shall be recorded solely by appending a new event.
(d) **Correction Authority**.—
(1) No correction or amendment event may be appended to a patient's event ledger without the cryptographically signed consent of the patient (or their authorized representative).
(2) An amendment event must be cryptographically signed by either:
(A) the individual practitioner who signed the original care event;
(B) a practitioner holding equivalent or superior professional credentials in the relevant clinical specialty; or
(C) an authorized institutional clinical audit board following a documented dispute resolution process.

TITLE III—LEGACY SILO WRAPPER STANDARDS

SEC. 301. PLUG-AND-PLAY SILO WRAPPER INTEGRATION.

(a) **In General**.—Health care providers operating legacy relational database Electronic Health Record systems shall not be required to replace their core databases, provided that they deploy an API Facade and translator wrapper layer, known as a **Plug-and-Play Silo Wrapper**.
(b) **Wrapper Capabilities**.—The Silo Wrapper shall:

(1) Intercept outbound legacy HL7 v2 and FHIR REST clinical events, translate them into the unified JSON event schemas established under Title II, sign them with the provider's cryptographic key, and append them to the universal ledger via gRPC.
(2) Monitor the patient's ledger stream via Kafka or equivalent event broker, translate new ledger entries into HL7 or FHIR resources, and write them back to the legacy relational EHR database.

TITLE IV—ASYNCHRONOUS ADMINISTRATIVE DECOUPLING AND FAULT ISOLATION

SEC. 401. COMMAND QUERY RESPONSIBILITY SEGREGATION (CQRS).

(a) **Silo Isolation**.—The clinical write-path (Command) and the administrative read-path (Query) of all health information networks shall be permanently decoupled.
(b) **Clinical Write-Path Performance**.—The clinical write-path shall write directly to the patient event ledger and shall have zero runtime dependency on prior authorization systems, payer gateways, coding validation engines, or insurance eligibility systems.
(c) **Clinical Care Unaffected by Billing Disputes**.—No validation failure, formatting error, payer API outage, or prior authorization dispute shall delay, degrade, or prevent the clinical recording of care or the delivery of care to the patient.

SEC. 402. FAULT ISOLATION AND CIRCUIT BREAKER MANDATE.

(a) **Clearinghouse Facade Circuit Breakers**.—All billing entities and clearinghouses shall implement automated Circuit Breaker systems on all outgoing administrative claims pipelines.

(b) **Dead Letter Queue (DLQ) Redirection**.—

(1) Any administrative transaction or billing projection that fails schema validation, ICD-10/CPT coding alignment, or insurance eligibility checks shall be isolated into a Dead Letter Queue (DLQ).

(2) The diversion of a failed claim to a DLQ shall not delay, freeze, or hold up the payment of undisputed claims, and shall not impact patient care or access.

(c) **Service Level Agreement for DLQ Resolution**.—

(1) Any administrative claim diverted to a DLQ must be audited, adjudicated, and resolved by the responsible health insurance issuer or payer within 30 calendar days of the initial diversion.

(2) If a payer fails to resolve a DLQ claim within the 30-day period, the claim shall be deemed approved and payable in full, and shall accrue statutory interest at a rate of 1.5 percent per month until paid.

SEC. 403. RELEGATION OF PRIOR AUTHORIZATION TO DOWNSTREAM READ-LOOPS.

(a) **Asynchronous Prior Authorization**.—All automated prior authorization rules, insurance policy evaluations, and coverage determinations shall execute in downstream, asynchronous read-loops reading from the patient's Kafka event stream.

(b) **Elimination of Point-of-Care Delay**.—Payer networks are prohibited from requiring synchronous authorization prior to the clinical execution of an order. The clinical order event is written instantly; the payment coverage dispute is resolved asynchronously.

SEC. 404. MEDICAL LOSS RATIO ALIGNMENT AND PREMIUM REDUCTIONS.

(a) **In General**.—The Secretary, in consultation with the National Association of Insurance Commissioners (NAIC), shall amend federal Medical Loss Ratio (MLR) requirements established under section 2718 of the Public Health Service Act to

account for UHAEP transaction and administrative labor efficiencies.

(b) **Mandatory Rebates and Premium Reductions**.—Health insurance issuers that achieve administrative cost savings as a result of UHAEP implementation shall reallocate such savings to direct patient care services or quality improvement activities. Any issuer that fails to meet amended MLR thresholds due to administrative savings shall issue annual premium rebates to enrollees in proportion to the savings achieved, ensuring that UHAEP efficiencies directly lower consumer healthcare premiums.

TITLE V—ENFORCEMENT, PENALTIES, AND FUNDING

SEC. 501. CIVIL AND CRIMINAL PENALTIES.

(a) **Prior Authorization Delays**.—Any health insurance issuer or payer that violates Section 403 by requiring synchronous blocking prior authorization, or delaying care delivery due to billing disputes, shall be subject to a civil monetary penalty of not less than $50,000 per occurrence.

(b) **Historical Ledger Alteration**.—Any software vendor, provider administrator, or individual who alters, overwrites, deletes, or tampers with the immutable ledger history shall be subject to criminal prosecution, and upon conviction, shall be fined not more than $250,000, or imprisoned for not more than 5 years, or both.

SEC. 502. AUTHORIZATION OF APPROPRIATIONS.

There are authorized to be appropriated such sums as may be necessary to carry out this Act, including grants to community health centers and rural hospitals for the implementation of Plug-and-Play Silo Wrappers.

SEC. 503. SAFE HARBOR AND INDEMNIFICATION FOR STANDARDS-DEVELOPERS AND OPEN-SOURCE CONTRIBUTORS.

(a) **Safe Harbor**.—No standards development organization, open-source software contributor, architect, designer, or system engineer who compiles, drafts, publishes, or distributes the technical specifications or reference implementations of the

Universal Health Architecture and Exchange Protocol (UHAEP) shall be subject to civil liability, administrative penalty, or regulatory action for any data breach, security failure, clinical error, or financial dispute arising from downstream deployment or modification of the protocol by clinical providers, payers, clearinghouses, or EHR vendors.

(b) **Preemption of State Law**.—The provisions of this section shall preempt any State or local law that imposes liability on software designers or standard-setting entities for downstream implementations of certified federal health information exchange standards.