Patient Identity Through Behavioral Continuity

by Nick Clark | Published March 27, 2026 | PDF

Patient misidentification causes thousands of adverse events annually because healthcare identity depends on wristbands, medical record numbers, and enrollment databases that fail at transitions of care. Keyless identity enables patient continuity through accumulated behavioral trajectory rather than stored identifiers, providing identity that strengthens with each clinical encounter and persists across institutions without centralized enrollment.

The identity failure at transitions of care

Patient identity errors in healthcare concentrate at transitions: emergency department admission, inter-facility transfer, handoff between care teams, and cross-institutional referral. Each transition involves a re-identification step where the patient must be matched to their records through identifiers that may be unavailable, incorrect, or ambiguous.

An unconscious patient arriving in an emergency department has no wristband, cannot provide a medical record number, and may not carry identification. A patient transferred between hospitals has a medical record number at the sending hospital that is meaningless at the receiving hospital. A patient who visits multiple health systems accumulates multiple identities with no structural mechanism to unify them.

The industry estimates that between 8% and 12% of patient records contain duplicate or mismatched identities. Each mismatch creates a risk of wrong-patient treatment, medication errors, missed allergies, or repeated diagnostic procedures. The financial cost is measured in billions. The human cost is measured in preventable harm.

Why centralized patient matching cannot eliminate the gap

Master Patient Index (MPI) systems attempt to resolve duplicates through probabilistic matching of demographic data: name, date of birth, address, and social security number. These algorithms achieve useful accuracy within a single institution but degrade significantly across institutions where data quality, data formats, and data completeness vary.

National patient identifier proposals would solve the matching problem but face political, privacy, and practical obstacles. A single identifier for every patient creates a surveillance and breach risk that many stakeholders consider unacceptable. The identifier must be issued, managed, and secured by some central authority, creating the same single-point-of-failure risk that credential databases present in financial services.

Biometric matching using fingerprints or palm vein scans improves accuracy but creates stored biometric templates that are subject to breach and cannot be revoked. A patient whose biometric template is compromised cannot change their fingerprints. The biometric approach trades one stored-secret vulnerability for another that is permanent.

How keyless identity addresses this

Keyless identity derives patient identity from accumulated behavioral continuity across clinical encounters. There is no stored template, no central identifier, and no enrollment database. Instead, each clinical encounter extends a dynamic hash chain that captures the patient's identity trajectory through locally-sourced signals: physiological characteristics, interaction patterns, device associations, and clinical context.

The trust slope validates patient identity through consistency of this trajectory over time. A patient who has accumulated multiple clinical encounters has a strong trust slope that is difficult to forge because each link in the chain depends on entropy sources specific to the actual patient at the actual time of the encounter. An attacker would need to replicate not just a snapshot of the patient's identity but the entire accumulated trajectory.

For emergency patients without prior encounters, the system begins building a trust slope from the moment of admission. Physiological signals from monitoring devices, interaction patterns with clinical staff, and environmental characteristics begin forming the identity trajectory. By the time the patient is transferred or discharged, a usable trust slope exists that can be validated at the next encounter.

What implementation looks like

A healthcare system deploying keyless patient identity integrates trust slope validation into existing clinical workflows. Bedside monitors, clinical devices, and nursing interactions all contribute to the patient's continuously evolving identity trajectory. No separate enrollment step is required. Identity emerges from the clinical encounter itself.

For inter-facility transfers, the patient's trust slope transfers with them. The receiving facility validates the slope against the patient's current physiological and behavioral signals. If the signals are consistent with the accumulated trajectory, the identity is confirmed without requiring the sending facility's medical record number, a central patient matching service, or manual re-identification.

For cross-institutional encounters, the trust slope provides a structural mechanism for patient matching that does not depend on demographic data quality or probabilistic algorithms. The identity is validated through behavioral continuity, not through comparison of stored attributes that may be incomplete or inconsistent.

For patient safety, keyless identity reduces misidentification risk because the identity is continuously validated through the patient's own behavioral and physiological trajectory. A wristband can be placed on the wrong patient. A medical record number can be mistyped. A behavioral trajectory that has accumulated over multiple encounters is structurally resistant to these error modes.

Keyless Identity All 21 steps →

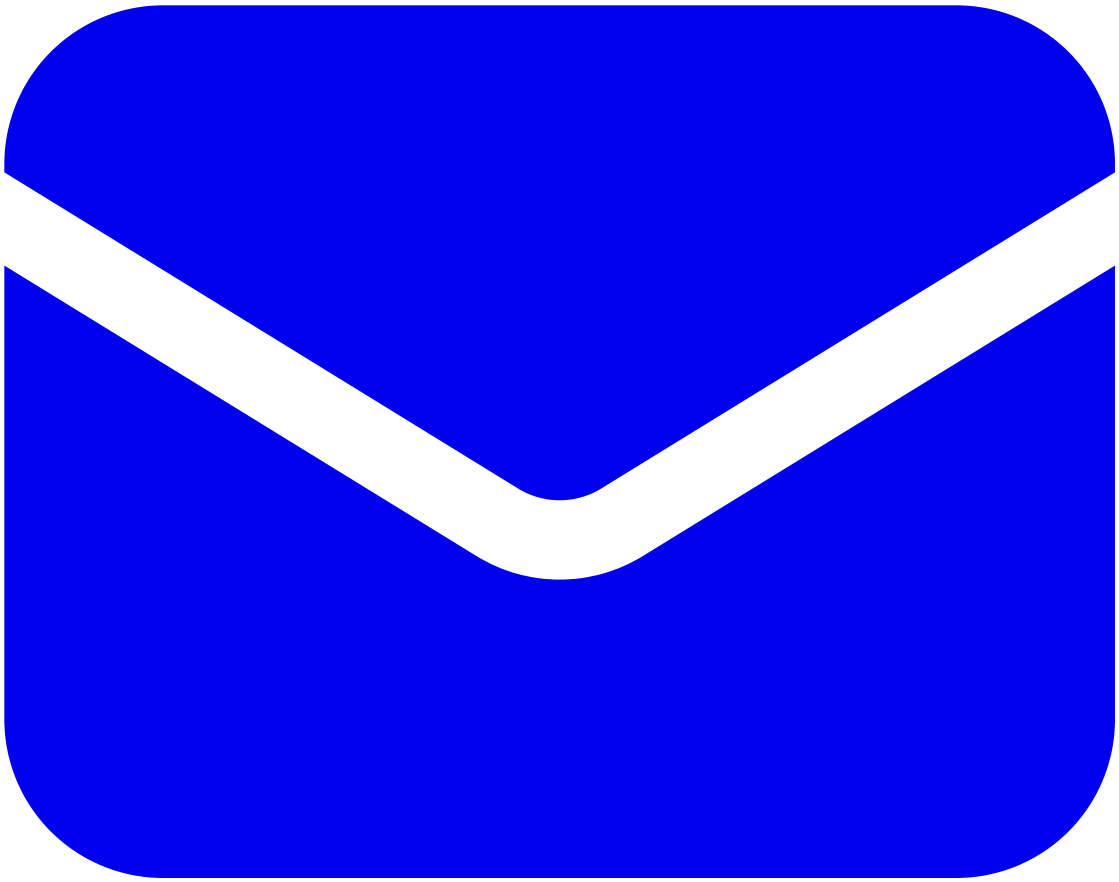
Identity from accumulated continuity. Post-quantum by construction.

Patent
US 19/388,580 · published
Primary Technical Disclosure
○ Stateless Device Pseudonymity and Secure Messaging in Cognition-Native Systems
Secondary Technical
○ Continuity-Based Biological Identity Using Trust-Slope Validation○ Trust Slope as Identity Primitive: Cumulative Hash Chains Replace Static Credentials○ Dual-Source Identity Derivation: Hardware Anchors and Local State Vectors Combined Per Epoch○ Stateless Symmetric Encryption: Session Keys Derived From Current Identity State○ Two-Stage Message Authentication: Transport Continuity Screening Before Semantic Validation○ Agent-Substrate Slope Entanglement: Binding Every Mutation Step to Its Execution Host○ Append-Only Mutation Lineage Log: Forward-Secure Identity Transition Chains○ Cumulative Slope Validation Across Substrates: Multi-Node Provenance Verification○ Quorum-Based Identity Recovery: Peer Attestation After Memory Loss○ Entropy Anchor Rotation: Proactive Identity Reseeding With Forward Links○ Biometric-Assisted Reseeding: Privacy-Preserving Fuzzy Extractors for Anchor Rotation○ Delayed Slope Validation: Bounded Proof Windows for Disconnected Environments○ Sparse Trust Slope Recovery: Compact Checkpoints for Resource-Constrained Devices○ Predictive Identity Validation: Drift Detection Before Full Discontinuity○ Legacy PKI Fallback: Session-Scoped Adapters With Strict Isolation Boundaries○ Post-Quantum Alignment: Hash-Based Security Without Vulnerable Hardness Assumptions
Applications (General)

○ Trust Slope Entanglement: Cryptographic Lineage for Semantic Agents○ Post-Quantum Enterprise Identity Migration○ Billions of IoT Devices Need Authentication Without Keys○ Financial Identity Without Credential Databases● Patient Identity Through Behavioral Continuity○ Supply Chain Authentication Without PKI○ Smart Building Access Through Continuity○ Vehicle Operator Identity Binding○ Displaced Person Identity Without Documents
Applications (Specific)
○ Okta Centralized Enterprise Identity. The Keys That Prove It Are Still Stored Somewhere.○ Auth0 Made Developer Identity Easy. The Credential Model Underneath Did Not Change.○ YubiKey Made Hardware Authentication Practical. The Key Is Still the Vulnerability.○ CLEAR Made Airport Identity Fast. It Built a Biometric Database to Do It.○ Worldcoin Scans Irises to Prove Humanity. The Proof Depends on a Central Enrollment System.○ Jumio Automated ID Verification. The Verification Still Depends on Documents.○ Microsoft Entra Unified Cloud Identity. Identity Still Depends on Stored Credentials.○ Ping Identity Built Enterprise Federation. The Federation Depends on Shared Secrets.○ OneLogin Simplified Enterprise SSO. The SSO Token Is Still a Credential.○ Duo Security Made MFA Ubiquitous. The Second Factor Is Still a Credential.○ Thales HSMs Protect Key Material. The Keys Still Exist.○ Entrust Issues Digital Certificates. The Certificate Is a Stored Credential.○ DigiCert Secures the Web With TLS Certificates. The Certificate Model Has Structural Limits.○ Let's Encrypt Made TLS Free. The Certificate Model Is Still the Same.
Keyless Identity overview →
AQ
deterministic
autonomy

Legal

Last updated: 2026-03-03



-
- nick@qu3ry.net
- 72 28 14 36 01

Invented by Nick Clark | Founding Investors: Devin Wilkie