# PROVISIONAL PATENT APPLICATION

## Systems and Methods for Quantum Privacy-Enabled Personalized, Value-Based Universal Exchange for Better Health

**Provisional Filing Date**: November 27, 2025

**Inventors**: Jonathan Paul Hare (CEO), Richard Arthur Muth (CTO)

**Applicant/Assignee**: WebShield, Inc. (Delaware)

### ABSTRACT

The invention provides systems and methods for enabling personalized, value-based healthcare through a unified, privacy-preserving computational and coordination infrastructure. The disclosed Quantum Privacy Network (QPN) employs Quantum Privacy Cells (QPCs), Privacy Domains, Trust Blocks, Trust Criteria, Proof-of-Trust (PoT) attestations, and EasyAccess workflow threads to support secure, compliant, real-time coordination among patients, clinicians, caregivers, enterprises, payers, manufacturers, public-health authorities, and autonomous AI agents without exposing protected health information (PHI) or proprietary enterprise data.

Computation is executed within cryptographically bounded Privacy Domains in which data, rights, obligations, and policies remain inseparably bound to Trust Blocks that persist across all transformations, aggregations, and downstream workflows. QPN thereby enables privacy-preserving analytics, zero-knowledge eligibility determinations, cross-organizational workflow orchestration, and multi-sponsor settlement without requiring data centralization or modification of existing enterprise systems.

The invention further provides systems and methods for dynamic benefit design, personalized care pathways, automated prior authorization, medication management, outcomes-based contracting, population-health surveillance, clinical research participation, and cross-sector incentive alignment. Personalized AI health agents operate within QPCs to deliver real-time navigation, risk forecasting, preventive-care recommendations, and continuous optimization of clinical, behavioral, financial, and environmental factors.

Through this architecture, the invention establishes a self-funding, privacy-preserving, person-centered universal exchange for health and well-being. The resulting system unifies care delivery, benefits, payments, public health, patient safety, and research into a single AI-optimized fabric capable of improving outcomes, reducing costs, and enabling equitable, population-scale personalized healthcare.

# Table of Contents

## CROSS-REFERENCE TO RELATED APPLICATIONS

This application relates to U.S. Patent Application **No. 19/206,859**, filed **May 2025**, titled "*Quantum Privacy, Proof of Trust, and Privacy Network Exchange*," which itself is a **Continuation-in-Part** of **U.S. Patent No. 12,316,610 B1**, titled "*Privacy Network and Unified Trust Model*."

This application further **claims the benefit of priority under 35 U.S.C. § 119(e)** to the following U.S. **Provisional Patent Applications**, each incorporated by reference in its entirety:

- U.S. Provisional Patent Application No. **63/804,583**, filed **May 12, 2025**, titled "*Quantum Privacy, Proof of Trust, and Privacy Network Exchange*";
- U.S. Provisional Patent Application No. **63/895,861**, filed **October 7, 2025**, titled "*Systems and Methods for Trust-Verified Tokenization & Settlement*"; and
- U.S. Provisional Patent Application No. **63/923,253**, filed **November 22, 2025**, titled "*Systems and Methods for Quantum Privacy-Enabled Self-Funding AI Trust, Safety & Compliance*."
- Applicant further anticipates filing a related U.S. Provisional Patent Application titled "*Systems & Methods for a Self-Funding, Self-Organizing Quantum Privacy Exchange*

*and Accelerator Network*" on or about **November 29, 2025**, to which one or more subsequent continuation-in-part applications may claim priority.

All of the foregoing applications are **commonly assigned to WebShield, Inc. (Delaware)** and are **incorporated by reference** for purposes of **priority and enablement**.

## FIELD OF THE INVENTION

The present invention relates to systems and methods for privacy-preserving computation, multi-party workflow orchestration, and personalized health optimization operating across clinical, financial, behavioral, environmental, and consumer-digital ecosystems.

More particularly, the invention concerns a Quantum Privacy Network (QPN) and Privacy Network Exchange (PNX) that use Quantum Privacy Cells (QPCs), Privacy Domains, Trust Criteria, Trust Blocks, Proof-of-Trust (PoT), and cross-sector EasyAccess workflow threads to enable secure, compliant, real-time coordination among patients, clinicians, caregivers, enterprises, manufacturers, payers, public-health authorities, digital services, and autonomous AI agents.

The invention spans three interdependent domains:

1. **Privacy-Preserving Computation & Governance:**
   Architectures that enforce cryptographically bounded lawful computation, federated policy inheritance, multi-jurisdictional compliance, zero-knowledge analytics, deterministic auditability, and cross-party rights enforcement, without exposing protected health information (PHI), behavioral signals, or proprietary enterprise data.
2. **Personalized, Patient-Centered Healthcare & Benefits Optimization:**
   Systems enabling real-time care coordination, benefit design, therapeutic access, payer-provider-manufacturer interaction, medication and safety workflows, continuous risk modeling, and personalized intervention pathways using QPC-verified signals spanning clinical, behavioral, environmental, social, and lifestyle domains.
3. **Cross-Sector Digital Ecosystems & Multi-Sponsor Value Networks:**
   Dual-use computational frameworks enabling privacy-preserving personalization, incentives, contracting, payment routing, settlement, and behavioral optimization across e-commerce, financial services, entertainment platforms, workplaces, transportation systems, public agencies, and autonomous AI environments—without sharing sensitive data or compromising compliance.

The invention creates a unified, self-funding, AI-optimized universal exchange for health and well-being, in which computation moves securely to where data resides, workflows operate across multiple institutions without backend changes, and value-aligned incentives propagate across sectors under cryptographic control. The disclosed systems support autonomous personal health agents, cross-ecosystem engagement graphs,

environment-adaptive interventions, population-scale early-warning systems, multi-sponsor settlement, and pervasive AI governance and safety mechanisms.

In all embodiments, computation is executed within QPN-enabled infrastructure comprising QPCs, Privacy Domains, Trust Blocks, Trust Criteria, PoT, and EasyAccess workflow threads. Together, these mechanisms provide the technical foundation required to support nationwide personalized healthcare, cross-sector economic integration, multi-agent AI systems, and universal privacy-preserving digital services.

## 1.0 INTRODUCTION AND BACKGROUND OF THE INVENTION

The United States has spent decades—and trillions of dollars—attempting to build a patient-centered, personalized, value-based healthcare system. Yet despite vast investments in EMRs, cloud platforms, digital health tools, interoperability standards, and AI, the system remains fragmented, expensive, and chronically inefficient. Every stakeholder—patients, clinicians, employers, regulators, and innovators—feels this dysfunction daily.

**The problem is not a lack of effort, technology, or motivation. It is architectural.**

Healthcare today runs on a patchwork of incompatible systems: payer silos, PBM rails, fragmented portals, proprietary APIs, EHR ecosystems, claims processors, authorization hubs, clearinghouses, data brokers, and countless duplicative vendor networks. These systems were not designed to support real-time, personalized decisions, continuous care coordination, long-running cross-organizational workflows, or AI-optimized pathways. They cannot unify clinical data with benefits data, pharmacy data, genomics, social determinants, behavioral patterns, lifestyle indicators, or device telemetry. They cannot perform privacy-preserving computation, enforce trust across institutions, or align incentives in real time.

As a result, the healthcare system behaves as if it were **five separate industries**—care delivery, payments and benefits, public health, clinical research, and patient safety—each operating on its own rails and each reconstructing partial, context-poor replicas of the same individuals. This fragmentation is artificial. It is unnecessary. And it is catastrophic.

- Patients experience disjointed care.
- Clinicians face impossible administrative burdens.
- Patients, Employers & taxpayers pay more than any other nation for worse outcomes.
- Researchers struggle to access the data needed to discover & validate new therapies.
- Public-health agencies operate with slow, incomplete, or erroneous signals.
- And regulators must enforce laws that the underlying technology cannot support.

**Healthcare has proven nearly impervious to meaningful reform because the incumbents across all sectors have co-evolved to *profit from the dysfunction itself*.** Over decades, layers of contractual restrictions, misaligned incentives, opaque pricing structures, and incompatible IT systems have hardened into a self-reinforcing architecture that extracts value rather than creates it.

The dysfunction is not incidental—it is structurally embedded: in the business models, in the data silos, in the claims rails, in the administrative workflows, in the reimbursement rules, and in the software that defines how every participant must interact. This deeply rooted system rewards fragmentation, penalizes coordination, and makes it nearly impossible for innovations that benefit patients to reach scale. The consequences are borne not by the entities creating the friction, but by the patients who suffer, the clinicians who burn out, and the employers and taxpayers who finance the world's most expensive—and least coherent—health infrastructure.

The **Quantum Privacy Network (QPN)** finally solves this structural failure.

QPN enables privacy-preserving computation, cross-organizational orchestration, federated governance, multi-party trust enforcement, and AI-optimized decision support—all without exposing data or requiring backend changes. It unifies all participants through Personal Privacy Networks (PPNs) and Enterprise Privacy Networks (EPNs), enabling seamless interaction among patients, clinicians, caregivers, payers, PBMs, pharmacies, labs, manufacturers, and research networks.

Most importantly, the Quantum Privacy Network enables—for the first time—a **consumer-driven, self-funding, privacy-preserving, person-centered health exchange and marketplace**. Every workflow QPN automates (clinical, administrative, financial, research, public health, or behavioral) produces high-value, real-time, context-rich data and intelligence that can be reused across all domains of health at zero marginal cost. This makes the system sustainable, scalable, fair, and vastly more efficient.

This provisional patent describes **why nationwide personalized healthcare is effectively impossible without the Quantum Privacy Network**, and how QPN can transform healthcare into a unified, AI-optimized system capable of improving outcomes, lowering costs, and **increasing healthcare productivity by 30–50%.**

## 2.0 WHY EXISTING SYSTEMS ARE INCAPABLE OF SUPPORTING PERSONALIZED HEALTH

Delivering personalized, value-based healthcare requires continuous, real-time access to a unified evidence graph spanning:

- PHI and EMR data
- pharmacy and benefits data
- claims and billing records
- genomics and biomarker data
- social determinants and behavioral patterns
- consumer data
- environmental exposure signals
- financial eligibility and accumulator status
- provider performance and outcomes
- real-time engagement data
- device telemetry
- AI model outputs and risk assessments

No existing system—EMRs, HIEs, payer platforms, PBM systems, cloud analytics, interoperability frameworks, or AI tools—can compute safely across all these data classes without violating privacy laws, breaching contractual restrictions, or centralizing data in ways that are inherently insecure and non-compliant.

Current systems cannot support:

- privacy-preserving multi-source computation
- cryptographically bounded cross-stakeholder workflows
- zero-knowledge eligibility, risk scoring, or analytics
- immutable, multi-party lineage of incentives, rights, and obligations
- multi-jurisdiction constraint inheritance
- continuous, longitudinal coordination across organizations
- real-time agentic navigation or autonomous care orchestration

Interoperability frameworks like FHIR and TEFCA still require centralized data pooling or institutional "ownership" of data flows. This makes key use cases—behavioral health integration, genetic privacy, cross-payer care continuity, consumer-generated data, AI governance, and multi-party consent—impossible to implement safely or efficiently.

The result is a system in which:

- **care pathways** are disconnected
- **incentives** are misaligned
- **data** is fragmented and out of context
- **workflows** cannot cross institutional boundaries
- **patients** receive contradictory or incomplete guidance
- **clinicians** are overloaded with administrative complexity

- **costs** explode while outcomes stagnate

Personalized healthcare is not achievable on this infrastructure.

## 3.0 THE QUANTUM PRIVACY NETWORK: ENABLING PERSONALIZED, VALUE-BASED HEALTHCARE

Personalized, value-based healthcare requires something the U.S. system has never possessed: a unified, privacy-preserving computational fabric capable of coordinating many independent organizations while simultaneously protecting sensitive information, enforcing rights and obligations, and aligning incentives in real time. The Quantum Privacy Network (QPN) provides this missing foundation.

At its core are **Quantum Privacy Cells (QPCs)**—cryptographically bounded execution environments that allow computation to occur wherever the data resides, without moving, revealing, centralizing, or replicating it. Instead of extracting PHI into enterprise data lakes or transmitting it across APIs, QPN brings computation to the data inside personal or enterprise Privacy Domains that operate entirely under machine-enforced Trust Criteria. Within these domains, computation is insulated from privileged insiders, cloud administrators, enterprise operators, platform owners, and even AI vendors, while still enabling rich multi-stakeholder workflows.

But QPN goes far beyond secure enclaves. It introduces a **cryptographic trust architecture** that binds rights, obligations, provenance, policies, and usage constraints directly to data and ensures those bindings persist through every step of computation, transformation, aggregation, or downstream analysis.

### Cryptographically Bounded Trust: Trust Criteria, Trust Credentials & Immutable Trust Blocks

Every datum entering QPN is wrapped in a **Trust Block**—a cryptographically sealed, tamper-resistant envelope that encodes provenance, custodial lineage, contractual and regulatory constraints, jurisdictional rules, safety requirements, allowed transformations, and the precise authority of each participant. These Trust Blocks are linked into a Proof of Trust Graph, recording an indelible history of decisions, obligations, and conditions, including those inherited from upstream data sources.

As computation proceeds, **all outputs inherit the Trust Criteria** of every input they depend on, whether directly or indirectly. This inheritance makes provenance and rights self-enforcing. Constraints cannot be removed, obligations cannot be bypassed, and policy rules remain attached to the data and to every derivative produced from it. The

result is a system where lawful computation is cryptographically guaranteed—not dependent on institutional goodwill, organizational boundaries, or human oversight.

## Privacy Algorithms & Privacy Pipes: Transforming Data Into Provably Opaque, Computable Form

QPN also introduces a new class of secure data-handling mechanisms: **Privacy Algorithms** and **Privacy Pipes**. These components transform data and its bound Trust Credentials into forms that are **provably opaque and meaningless** to unauthorized parties, yet remain fully computable for authorized workflows. Data can be selectively reversed into clear text only when *every* Trust Criterion from *every* relevant stakeholder is satisfied.

This means encrypted or obfuscated data can be pooled, linked, aggregated, recombined, transmitted across jurisdictions, used in population-scale analytics, or incorporated into cross-sector workflows—while remaining cryptographically protected at all times. Even when millions of data points converge to generate a single decision-support output, that output inherits the Trust Criteria of all contributing inputs, ensuring that no unauthorized disclosure can occur.

In practice, most computations require no clear-text output at all. QPN natively supports zero-knowledge eligibility checks, privacy-bounded classification, minimal-disclosure interactions, encrypted analytics, and selective-personalization pathways that reveal only the specific result a workflow is authorized to use.

## Decentralized Privacy Domains & Distributed QPCs

Unlike traditional architectures that rely on centralized data warehouses or platform-owned aggregates, QPN is a **fully decentralized constellation** of:

- **Personal Privacy Networks (PPNs)** for individuals, clinicians, and caregivers
- **Enterprise Privacy Networks (EPNs)** for providers, payers, pharmacies, employers, labs, technology vendors, government agencies, and regulators
- **Cryptographically bounded Quantum Privacy Cells** operating inside each domain
- **Privacy Pipes** that connect domains through controlled, privacy-conscious pathways

Each Privacy Domain enforces its own rights and obligations. Every computation runs inside QPCs under strict cryptographic bounds. **Proof-of-Trust (PoT)** is executed before any computational step, verifying that all regulatory, contractual, clinical, and workflow constraints are satisfied.

This allows data and computation to safely flow across organizations, technologies, jurisdictions, and sectors—while ensuring that data leakage, privilege escalation, insider access, or unauthorized inference are mathematically impossible.

## Multi-Layer Protection: Absolute Proofs Against Data Leakage

QPN provides a level of privacy and cybersecurity that far exceeds traditional approaches. Its protection is multi-layered:

1. **Cryptographically bounded QPCs** prevent unauthorized access or exfiltration.
2. **Privacy Domains** isolate data based on legal, contractual, and jurisdictional constraints.
3. **Privacy Pipes** allows data to be linked or copied between privacy domains while remaining cryptographically under the control of their original sources.
4. **Privacy Algorithms** transform data into provably opaque yet computable formats.
5. **Trust Blocks** bind provenance, constraints, and obligations to all data and derivatives.
6. **Proof-of-Trust validation** ensures no information can be revealed or computation run unless fully compliant, regardless of where data flows or how it is transformed.
7. **EasyAccess Authorization** enables convenient, cross-organizational authorization with per-attribute, per-device, per-person, per-purpose access control.

These layers combine to enable **mathematically provable guarantees** that data cannot leak—not to a person, organization, system, device, cloud operator, AI model, or attacker. They eliminate privacy-versus-utility tradeoffs and enable safe, lawful, personalized computation at national and global scale.

This greatly simplifies computation and process integration – since policies are bound to data and automatically inherited, you can utilize data without thinking about privacy or security – since they are built into the network.

## Constitutional Protections for Patient-Controlled Privacy Domains

QPN's technical guarantees are reinforced by equally strong legal protections that safeguard patient-controlled data against compelled disclosure. Personal Privacy Networks (PPNs) operate as patient-controlled digital domains—not as HIPAA-covered entities, business associates, or institutional data custodians. Because of this, the data contained within a patient's Quantum Privacy Cell (QPC) enjoys the full spectrum of constitutional protections that apply to private spaces, private papers, and encrypted personal devices.

A QPC cannot decrypt or reveal patient data unless the patient explicitly authorizes it through the Trust Criteria bound to that data. This means that **the system itself is technically and cryptographically incapable of producing clear-text PHI in response to a subpoena, administrative demand, or law-enforcement request**. Any attempt to compel disclosure would necessarily require compelling *the patient* to authorize decryption.

Under longstanding Fifth Amendment doctrine, the government cannot force an individual to perform a "testimonial" act that reveals the contents of their mind—such as divulging a password, producing decrypted data, or otherwise enabling access to incriminating information. Courts have repeatedly held that compelling a person to decrypt or authorize access to encrypted personal information violates the Self-Incrimination Clause. Accordingly:

**Because the QPC cannot comply without patient authorization, and compelling the patient to authorize decryption would violate the Fifth Amendment, the system provides a legally enforceable form of irreversible privacy.**

Even where state law or political actors might attempt to obtain reproductive-health data, mental-health reflections, or sensitive behavioral information—such as records relating to sexual assault, substance-use history, or pregnancy outcomes—the PPN is not a covered entity and therefore **cannot be compelled under HIPAA's public-health or law-enforcement exceptions**. And because decrypting or reassembling the information requires the patient's own affirmative act, the individual can decline, and the government has no constitutional basis to compel cooperation.

In a very real sense, a patient's QPC stands in the same legal position as the patient's locked diary, encrypted phone, or private journal. If prosecutors attempt to force access, the constitutional barrier is the patient's own Fifth Amendment rights—not the technology itself. The QPC merely enforces those rights through unbreakable cryptography.

This absolute protection against compelled disclosure fosters a level of trust that is impossible in today's institutional systems. Patients can safely record, track, and manage their most sensitive information—addiction struggles, intrusive thoughts, trauma responses, emerging mental-health symptoms, reproductive concerns, financial stressors—knowing it can be used *only* to support them through anonymous decision support and safety workflows, and **never against them**. This trust is essential for enabling the early-warning, behavioral-health, and preventive-care capabilities that QPN makes possible at national scale.

Clinicians and provider organizations are legally obligated to retain only those records that they themselves create, rely upon, or incorporate into the official medical record for

purposes of clinical decisionmaking, legal compliance, quality assurance, or billing. Federal and state record-retention laws do not impose a duty to collect or store every piece of information a patient chooses to disclose. Instead, these laws require retention only of the provider's own work product—including clinical notes, diagnoses, treatment decisions, orders, and other entries formally incorporated into the medical record.

Under the Quantum Privacy Network (QPN), patients may maintain sensitive categories of information—including behavioral-health disclosures, reproductive-health information, trauma history, or real-time engagement signals—exclusively within their Personal Privacy Networks (PPNs). Clinicians may access this information ephemerally through clinician-specific PPNs authorized by the patient. These clinician PPNs allow the clinician to review patient-controlled information and to create clinical notes, diagnoses, and orders inside a cryptographically bounded environment, but they do not give the clinician possession of the underlying patient data or the ability to export or re-encode it into institutional systems unless explicitly authorized by the patient.

To satisfy federal and state record-retention requirements, QPN enables a provider-level records-retention service—also implemented through Privacy Domains and QPCs—to store the clinician's legally required documentation while keeping the patient's underlying data under the patient's exclusive control. The retained documentation includes the clinical note itself, the provider's reasoning, the orders given, and any relevant clinical conclusions, but not the raw patient-controlled data unless the patient elects to release it. This satisfies the provider's legal duties for malpractice defense, quality review, and regulatory compliance, while ensuring that identifiable patient-controlled information is never stored in provider-operated systems unless the patient expressly authorizes it.

Crucially, the provider and clinician do not have unilateral authority to disclose the patient's underlying PPN-controlled information. The provider record—although retained as required by law—is cryptographically bound to patient-controlled Trust Criteria that govern when identifiable disclosure is permitted. The provider may disclose only the de-identified or zero-knowledge components of those retained records for public-health, safety, surveillance, or quality-measurement functions unless the patient actively authorizes identifiable disclosure. If the patient seeks to bring a malpractice action or transfer identifiable records to another provider, the patient may authorize decryption and release through their PPN.

Because the underlying information remains under the patient's control—and because exporting or decrypting identifiable PHI requires an affirmative patient act—clinicians and provider organizations cannot be compelled under HIPAA, administrative subpoena, or state public-health or law-enforcement exceptions to produce identifiable PPN-hosted data. HIPAA applies only to PHI maintained by a covered entity or its business associates;

patient-controlled PPNs are neither. And compelling the patient to authorize decryption would constitute a compelled "testimonial" act that violates the Fifth Amendment's Self-Incrimination Clause under well-established doctrine.

Accordingly, the QPN architecture provides a legally robust dual-layer framework. Providers meet their statutory and regulatory record-retention obligations without acquiring or possessing sensitive patient-controlled information. Patients retain constitutional and technical control over their underlying PHI, ensuring that sensitive behavioral, reproductive, or personal data cannot be disclosed without patient consent. This framework satisfies clinical, regulatory, and malpractice-related documentation requirements while simultaneously enforcing constitutionally grounded, cryptographically guaranteed patient autonomy over identifiable information.

These constitutional protections reinforce—at the legal layer—the same guarantees that QPN enforces cryptographically at the technical layer.

## Clinician PPNs and Contractual Non-Disclosure Obligations

In certain embodiments, a clinician-specific Personal Privacy Network (PPN) and corresponding Quantum Privacy Cell (QPC) may be instantiated for each treating clinician, tethered to the patient's PPN and governed by the patient's Trust Criteria. When a clinician opts in to access the patient's Privacy Domain, that access occurs only through the clinician's QPC under a binding, machine-enforced service contract. By virtue of this opt-in, the clinician and provider organization enter into an enforceable agreement—cryptographically recorded in Trust Blocks—not to disclose or export any identifiable patient data without the patient's express authorization.

This contractually bound access pathway ensures that all cross-organizational data sharing, consultation, and care coordination proceed through EasyAccess authorization and PPN-to-PPN exchanges, maintaining end-to-end cryptographic privacy. The clinician may review patient-controlled information and generate clinical notes within the clinician QPC, but cannot re-encode or store identifiable patient data in institutional systems unless authorized by the patient. Because the contractual obligation is embedded directly into the clinician's Trust Criteria and cryptographically linked to every action taken within the clinician's QPC, the clinician gains an additional independent legal basis for declining coercive disclosure requests: not only are they technically incapable of producing clear-text PHI, but doing so would violate a binding contract to which they assented as a condition of access. This dual-layer protection—constitutional and contractual—creates a legally robust, technically enforced framework for safeguarding sensitive patient information while still enabling clinicians to deliver comprehensive, coordinated care.

## Zero-Knowledge Analytics & Minimal Disclosure Interaction

Because QPN makes both data and computation provably private, it can support a wide range of zero-knowledge workflows—such as real-time adjudication, cross-sector contracting, price transparency, public-health surveillance, lifestyle-signal modeling, and safety monitoring—without exposing PHI. Stakeholders receive the information they need (for example, "eligible," "safe," "allowed," "clinically appropriate," "high-risk," or "needs follow-up") without gaining access to the underlying data that informed the result.

This capability is essential for many of the systems described later in this invention, including personalized plan design, medication optimization, portable reinsurance, multi-sponsor incentives, national patient-safety networks, and privacy-preserving research systems.

## EasyAccess Workflow Threads & Cross-Organizational Coordination

QPN replaces the brittle, API-heavy interoperability paradigm with **EasyAccess workflow threads**—long-running, encrypted coordination channels that connect individuals, clinicians, payers, PBMs, pharmacies, labs, devices, digital therapeutics, employers, and community organizations.

These threads:

- run across systems that do not share APIs, data schemas, or identity systems,
- operate without backend changes,
- enforce multi-party Trust Criteria at every step,
- preserve full provenance and reversibility, and
- support seamless scheduling, referrals, prior authorization, care navigation, benefit optimization, payments, engagement, and follow-up.

They allow the healthcare system to behave as a single coordinated network—even though the underlying institutions remain independent and operate with their own technology stacks.

## From Fragmentation to a Unified, Person-Centered Network

When deployed at scale, the Quantum Privacy Network dissolves the maze of disconnected portals, platforms, data silos, identity systems, and proprietary rails that define today's healthcare ecosystem. It replaces them with a unified, intelligent, person-centered network in which:

- care becomes continuous instead of episodic,
- benefits become personalized instead of generic,
- coordination becomes proactive instead of reactive,
- AI becomes safe, auditable, explainable, and aligned with patient outcomes,

- incentives and payments become value-based and multi-sponsor,
- and individuals finally gain a system designed around their needs and preferences.

This architectural shift is what makes nationwide personalized healthcare—safe, compliant, efficient, and genuinely value-based—not only achievable, but inevitable. The demand for such a system is overwhelming; QPN is the first architecture capable of delivering it.

## 4.0 UNIFYING CARE DELIVERY, PAYMENTS, PUBLIC HEALTH, PATIENT SAFETY & RESEARCH

For more than fifty years, the U.S. healthcare system has evolved into five separate industries—care delivery, payments and benefits, public health, patient safety, and clinical research. Each domain built its own vendors, data warehouses, regulatory processes, business models, and incentive structures. Each created its own portals, APIs, message standards, clearinghouses, and administrative intermediaries. And each tries—independently—to reconstruct a partial, decontextualized view of the same people: patients, clinicians, caregivers, and their families.

Each sector of the healthcare system faces the same fundamental challenge: understanding a person's conditions, history, risks, environment, resources, preferences, and goals. Yet each sector attempts to solve this challenge from within its own institutional frame, using data that is incomplete, stale, inconsistently coded, or filtered through business and regulatory constraints.

Hospitals and clinicians see clinical data, but it is often narrow, episodic, and documented under time pressure. Payers receive clinical records in addition to claims, but these records are frequently delayed, error-prone, stripped of context, or distorted by billing requirements, fraud risk, or documentation incentives. PBMs have rich pharmacy data, but lack clinical nuance or context. Employers see benefits and utilization patterns, but not the real drivers behind them. Public-health agencies receive partial reports long after events occur. Researchers get retrospective, de-identified datasets that lack provenance and behavioral context. Safety agencies receive only adverse-event reports—usually late, incomplete, and inconsistently structured.

In every case, the information available is fragmented, delayed, incompatible, or tainted by conflicting incentives. No sector has a full, living, longitudinal understanding of the individual—and the institutional, contractual, and privacy barriers between sectors mean that none can safely or legally share what they know in real time. The result is a system where everyone is trying to care for the same person while no one has the complete or trustworthy picture needed to do so effectively.

The result is a national system that is:

- **Wasteful**, spending trillions on administrative burden and duplicated effort.
- **Dangerous**, producing avoidable harm due to missing context and delayed signals.
- **Expensive**, costing more than any system on Earth while delivering worse outcomes.
- **Demoralizing**, burning out clinicians, nurses, social workers, and care teams.
- **Inequitable**, underserving vulnerable communities and high-risk populations.
- **Ineffective**, despite extraordinary scientific and technological capabilities.

Industry incumbents—from PBMs to clearinghouses, data brokers, claims processors, and siloed EHR ecosystems—have learned to profit from this dysfunction. The fragmentation has been monetized, institutionalized, and contractually ossified. The people who suffer are patients, caregivers, clinicians, employers, taxpayers, researchers, and society itself.

The Quantum Privacy Network (QPN) and the Privacy Network Exchange (PNX) fundamentally change this architecture. They do not merely integrate these five domains—they reveal that they were *always one system*, artificially split apart by legacy constraints.

## National Multi-Ecosystem Health Utility Layer

QPN also enables a unified national "health utility layer" by establishing a common computational substrate that spans clinical, financial, public-health, patient-safety, research, and consumer domains. This utility layer is implemented through a distributed network of QPCs operating under shared Trust Criteria, lineage policies, and Proof-of-Trust (PoT) enforcement rules. Each QPC can securely orchestrate multi-party workflows that involve data, rights, obligations, and computational logic originating from multiple institutions and industries.

Through EasyAccess workflow threads, QPN supports the creation of cross-sector workflows that combine, for example, clinical diagnostics with real-time benefits adjudication; behavioral-risk indicators with public-health alert thresholds; medication-adherence stability with personalized contracting logic; or lifestyle-signal trajectories with clinical-trial eligibility. All workflow steps are executed inside QPCs, which enforce cryptographic constraints on data movement, permissible computations, jurisdictional requirements, contractual obligations, and patient permissions.

Because the same privacy-preserving computational fabric is used for care delivery, benefit logic, safety systems, AI governance, public-health analytics, and research execution, the network ensures semantic and operational consistency across all workflow types. This establishes a unified national rails architecture where every sector contributes value and benefits from shared intelligence—without sharing raw data or compromising privacy.

## A Person-Centered, Self-Funding Exchange That Unifies Healthcare

The Quantum Privacy Network makes it possible— for the first time— to unify care delivery, payments, public health, patient safety, and clinical research within a single, privacy-preserving, AI-optimized, self-funding national exchange.

Inside the QPN, every clinical, financial, behavioral, environmental, or research interaction occurs within Quantum Privacy Cells (QPCs), generating real-time, privacy-preserving, cryptographically verified data with complete provenance and context. This data is:

- **more accurate** than claims or retrospective registries,
- **more complete** than siloed EHR or PBM systems,
- **more actionable** than traditional analytics,
- **more trustworthy** due to cryptographic lineage, and
- **more reusable** than any other health-data asset.

And because all five domains depend on the same underlying information about the same people, **any improvement or automation in any one domain automatically generates the evidence, computation, and patterns needed by all the others—at zero marginal cost.**

This is the core breakthrough: QPN turns healthcare's long-standing inefficiencies into a virtuous cycle of continuous improvement, where value generates more value and intelligence in one area immediately strengthens the others.

## Zero-Marginal-Cost Reuse of Data, Infrastructure & Computation

Every workflow that QPN automates—prior authorization, medication therapy management, referrals, price transparency, benefit optimization, social-needs interventions, public-health surveillance, safety monitoring, clinical-trial matching—produces a rich set of reusable assets:

- clean, validated, context-rich data,
- real-time engagement events from patients and clinicians,
- cryptographically verified provenance,
- reusable analytics inputs,
- privacy-bounded model outputs,
- agent-generated reasoning trails, and
- fully authorized computation histories.

In today's healthcare ecosystem, each of these artifacts would require a separate data-sharing agreement, integration, vendor contract, compliance review, and bespoke analytics pipeline.

Inside QPN, they are **produced automatically**, under uniform trust constraints, with cryptographic compliance, and become immediately available—at zero marginal cost—to all authorized stakeholders.

This is not a theoretical "data lake." It is a real-time, distributed, privacy-preserving evidence graph that grows richer with every interaction. **The Privacy Network Exchange enables this evidence graph – along with the engagement of patients, clinicians, and caregivers – to be reprocessed, reanalyzed, recombined, and reused across all sectors of healthcare** without compromising privacy, cybersecurity, regulatory compliance, or any participant's commercial rights.

This converts the entire industry's current fragmentation and inefficiency into a self-funding engine for continuous improvement.

## Federated Lifestyle-Signal & Engagement Graphs

The Privacy Network Exchange allows each QPC to generate and maintain a federated, continuously updated lifestyle-signal graph derived from user interactions across multiple domains—clinical encounters, medication events, financial-stress indicators, mobility patterns, digital-media engagement, food and retail choices, workplace interactions, caregiver-supported tasks, and device telemetry. All signals are ingested in encrypted form within the user's Privacy Domain and are tagged with cryptographically verifiable provenance attributes, regulatory lineage flags, and Trust Criteria contributions from clinicians, caregivers, employers, or public-health authorities.

Because QPCs enforce per-signal computational constraints, they can execute privacy-preserving risk-scoring, trajectory projection, anomaly detection, behavioral-pattern stability analysis, nutritional/environmental exposure modeling, or stress-tolerance modeling without revealing the signals to any outside party. Outputs—such as elevated-risk markers, safety-threshold warnings, eligibility determinations, or personalized plan adjustments—are computed in zero-knowledge form. This ensures they can be selectively disclosed only to authorized participants, such as the user, a clinician, a decision-support tool, or a payer's plan-design logic.

The federated design eliminates the need for centralized behavioral databases or cross-institutional data pooling. Instead, each PPN continuously recomputes its engagement graph locally while exchanging only privacy-bounded outputs with the network. Through Quantum Privacy, a patient's decentralized Personal Privacy Network can reconnect records about the patient across disparate organizations and systems, protecting them all within the virtual boundaries of their personal Privacy Domain and Quantum Privacy Cell. These outputs become reusable computational inputs for value-based plan design, medication therapy management, personalized contracting, care navigation, clinical

research eligibility, and public-health trend detection—thereby providing substantial cross-domain value with zero marginal cost.

## Transforming Healthcare into a Unified Patient-Centered Ecosystem

- **Care Delivery:** QPN connects EMRs, pharmacies, diagnostics, telehealth platforms, behavioral health, social care, and preventive services into a unified, context-rich coordination fabric. Clinicians, patients and caregivers finally receive real-time, complete, privacy-preserved insights—enabling better diagnoses, fewer errors, stronger continuity, and more personalized care.
- **Payments & Benefits:** Tokenized benefits, eligibility rules, accumulators, copay assistance, affordability logic, rebates, incentives, and real-time plan design all run on the same evidence base that powers clinical decision-making. This unifies financial and clinical pathways into a coherent, patient-centered experience.
- **Public Health:** Zero-knowledge epidemiology, environmental exposure detection, vaccination status insights, outbreak prediction, and community-level risk modeling become possible without exposing personal data or centralizing PHI. Public health becomes real-time, interactive, and personalized.
- **Patient Safety & Quality:** Every care episode, medication event, diagnostic step, and device interaction generates cryptographically immutable Trust Blocks capturing clinical context, safety signals, outcome trajectories, and AI governance lineage. Safety becomes continuous and nationwide.
- **Clinical Research:** Federated trial matching, automated consent, real-world evidence generation, protocol-embedded care tasks, and continuous CRAACO participation become seamlessly embedded in everyday care. Research evolves from episodic and siloed to real-time and universal.

In the QPN, all five sectors run on the same rails—with the same provenance, shared intelligence, and unified privacy infrastructure.

## Turning Dysfunction into Intelligence: How QPN Becomes Self-Funding

The current healthcare system loses trillions of dollars annually to:

- redundant documentation,
- duplicated tests,
- unnecessary treatments,
- delayed care,
- administrative overhead,
- manual data gathering,
- siloed analytics teams,

- opaque contracting layers, and
- expensive intermediaries.

QPN converts all of this dysfunction into self-reinforcing intelligence and reusable resources. Every point of friction QPN removes—every coordinated referral, every automated prior authorization, every optimized benefit, every medication intervention, every social-needs match, every safety detection—generates measurable, monetizable savings. Those savings directly fund further adoption, producing a compounding cycle of efficiency.

This is why QPN can expand nationally **without requiring new infrastructure spend from providers, payers, employers, or government agencies.** It is a self-funding transformation.

## Pooling Data and Intelligence Across Every Sector of the Economy

Health does not emerge from clinical systems alone. It is shaped by how people live, work, shop, learn, commute, communicate, play, and care for one another. Every employee, every customer, every student, every citizen is also a patient—regardless of whether they are actively receiving care.

The Quantum Privacy Network makes it possible to pool resources from and align incentives and behaviors across:

- e-commerce and consumer platforms,
- financial services,
- government programs,
- business-process automation systems,
- employer wellness initiatives,
- education systems,
- transportation platforms,
- lifestyle and entertainment ecosystems.

All of this occurs without surveillance, without data sharing, and without violating privacy or regulatory constraints. QPC-bounded computation ensures that every interaction—across every sector—can be used to improve health outcomes meaningfully and safely.

This creates the world's first **person-centered universal market**, where incentives, AI, benefits, and care pathways continuously learn and adapt to support better health as a natural by-product of daily life.

By unifying care delivery, payments, public health, patient safety, and clinical research into one self-funding ecosystem, the Quantum Privacy Network makes it possible to simultaneously improve care delivery, eliminate waste, protect privacy, empower

clinicians, democratize research, strengthen public health, align incentives, and accelerate AI optimization for everyone.

This transforms the healthcare system from fragmented siloes into a unified, person-centered network capable of delivering dramatically better outcomes at dramatically lower cost.

## Dual-Use Cross-Sector Infrastructure Integration

The QPN architecture also enables a novel method for utilizing existing digital-commerce, financial-services, consumer-online, entertainment, and enterprise-workflow infrastructures as dual-use computational resources for health-relevant processes. Rather than requiring the creation of new health-specific networks, QPN's design allows PPNs and Enterprise Privacy Networks (EPNs) to interface with the APIs, session flows, interaction patterns, and identity primitives that already exist in these non-health sectors.

Under this model, a PPN can carry out privacy-preserving, zero-knowledge interactions with external services to obtain real-time context such as product attributes, pricing, nutritional metadata, environmental factors, risk-relevant content categories, financial-stress indicators, or time-of-day patterns—without revealing any sensitive health data. QPCs then fuse this externally sourced context with internal health-linked Trust Criteria and multi-party provenance to produce actionable, privacy-bounded outputs. These outputs can include eligibility results, personalized recommendations, compliance-constrained incentives, or risk-adaptive pathways.

This integration mechanism allows QPN to reuse the existing infrastructure of sectors that already operate at massive scale—e-commerce catalogs, payments systems, transaction processors, digital advertising networks, device OS personalization layers, and media-selection engines—without requiring any modification to those systems. QPN merely uses the data and rights patients and clinicians already possess (e.g., device permissions, account credentials, purchase histories, family-sharing rights) as cryptographically bounded computational inputs. Because these sectors already have highly optimized distribution and personalization infrastructures, QPN's health-preserving computations can be performed at negligible marginal cost while maintaining strict regulatory, consent, and data-minimization requirements.

This dual-use integration converts the broader economy into a privacy-preserving behavioral-health, lifestyle-optimization, and environmental-risk-mitigation engine—without the underlying sectors learning or processing any PHI or risk-sensitive information.

## Privacy-Preserving Behavioral Optimization Across Everyday Digital Ecosystems

The Quantum Privacy Network further enables a set of privacy-preserving behavioral-optimization functions that operate automatically across all user-facing digital environments connected through the Privacy Network Exchange. Within each user's Personal Privacy Network (PPN), Quantum Privacy Cells (QPCs) continuously maintain a federated, provenance-bound engagement graph representing an individual's preferences, contextual risk indicators, environmental exposures, and authorized behavioral-health signals. These signals remain encrypted and never leave the individual's PPN; instead, QPCs execute personalization, recommendation, and incentive logic internally under machine-interpretable Trust Criteria contributed by clinicians, care teams, employers, public-health authorities, and the user.

Using this architecture, QPN is able to generate "healthy default pathways" that surface context-appropriate choices in real time. When a user interacts with a QPN-enabled ecosystem—such as e-commerce platforms, food-ordering services, financial-wellness tools, transportation apps, entertainment platforms, or workplace systems—the PPN performs a zero-knowledge interaction with the external service's authorization logic. This permits the external service to receive only the minimal eligibility or personalization signal necessary to tailor content, offers, recommendations, or risk mitigations, without learning any underlying health, behavioral, or lifestyle information.

QPN's internal policy engine can then apply distributed value-based nudges within the user's existing digital workflows. These nudges may include: adjusting result order to prioritize clinically favorable items or better value; generating context-aware EasyAccess incentives tied to healthy behaviors; suppressing offerings that conflict with risk thresholds; or activating micro-interventions (e.g., stress-reduction prompts, sleep-stability recommendations, caregiver alerts) when QPC-verified signals satisfy clinical criteria. All nudging and recommendation logic executes entirely within the user's Privacy Domain, ensuring that external systems cannot observe, infer, or reconstruct PHI, behavioral data, or risk indicators.

This cross-sector behavioral-optimization layer enables QPN to reinforce clinically valuable behaviors at zero marginal cost, using the digital environments people already engage with, while remaining fully compliant with privacy, regulatory, employment, and discriminatory-impact constraints.

## 5.0 REMOVING INTERMEDIARY FRICTION & PREVENTING DATA BLOCKING

The U.S. healthcare system contains entrenched intermediaries—PBMs, GPOs, payers, provider networks, clearinghouses, authorization hubs, pharmacies, and data brokers—whose business models depend on controlling data and workflow access.

These intermediaries impose rent-seeking friction through:

- data gatekeeping
- proprietary rails
- lock-in workflows
- administrative tolls
- distorted incentives
- anti-competitive blocking

The Quantum Privacy Network eliminates these barriers by ensuring:

- data remains within personal or enterprise privacy domains
- workflows operate "on top" of existing systems without backend changes
- data rights of patients and clinicians are automatically enforced, preventing data blocking by industry incumbents.
- incentives are cryptographically aligned
- trust verification is neutral and tamper-resistant
- incumbents cannot block access or manipulate workflows

This structural neutrality is essential for nationwide adoption.

## 6.0 Building Better Health into Daily Lives with Quantum Privacy

The Quantum Privacy Network (QPN) enables a fundamentally new kind of health infrastructure—one that expands organically, funds its own growth, and generates benefits that ripple far beyond the boundaries of healthcare.

Because QPN eliminates structural waste, reduces friction, and continuously improves coordination, every workflow it automates produces measurable economic value. These savings accumulate across stakeholders—providers, payers, employers, government agencies, patients, and their families—who can independently drive further adoption and savings. As value compounds, adoption accelerates without requiring new capital investments, disruptive system replacements, or top-down mandates.

A core reason this transformation is possible is that, instead of replacing enterprise systems or forcing adoption of new APIs, the **Quantum Privacy Network leverages dual-use infrastructure that uses the accounts, permissions, and workflow rights patients, clinicians, and organizations already possess**. Every new use case—clinical, financial,

administrative, or research—reuses the same privacy, identity, evidence, and computation infrastructure. This produces a scaling dynamic with **near-zero marginal cost**, allowing QPN to grow naturally as more participants and workflows join the network.

Over time, these person-centered privacy networks aggregate demand at national and global scale and enable personalized contracting relationships among manufacturers, employers, clinicians, and patients—something that was technologically or legally impossible before QPN. As adoption spreads, costs decline, outcomes improve, and the system strengthens itself through continuous reinvestment of savings.

## Health as an Emergent Property of Everyday Life

Most health outcomes are not determined inside hospitals or clinics. They emerge from the conditions in which people live, work, learn, shop, communicate, and entertain themselves. **Behavioral patterns, daily choices, food environments, sleep, stress, finances, social engagement, and digital consumption exert far greater influence on population health than episodic medical care.**

**Yet the healthcare sector—payers and providers alike—has almost no visibility into these determinants and no meaningful ability to influence them.** They cannot access the relevant data, shape the environments people interact with, or guide the moment-to-moment decisions that cumulatively determine long-term health.

The Quantum Privacy Network (QPN) and the Privacy Network Exchange (PNX) correct this structural limitation by extending the same privacy-preserving infrastructure that powers personalized care into the broader economy where people actually live their lives. The QPN architecture is inherently dual-use: the same cryptographic **Privacy Cells that enable compliant healthcare workflows can also support personalization, automation, incentives, and decision support across financial services, e-commerce, consumer online platforms, entertainment, business process automation, workplaces, and government services—without exposing any sensitive information or creating surveillance risk.**

Because these sectors already operate efficient, low-cost, highly scalable digital marketplaces, the QPN can reuse their infrastructure at zero marginal cost, while giving it bulletproof privacy, regulatory compliance, and patient-centered control. This makes it possible—for the first time—to integrate privacy-sensitive health contexts into environments that shape behavior billions of times per day. As people interact with digital commerce, payments, media, food ordering, workplace systems, transportation services, and community platforms, QPN can learn from those interactions (anonymously, with full provenance, and under user control) and deliver healthy defaults, personalized nudges, risk-reducing recommendations, and value-aligned incentives in real time.

## Behavioral and Environmental Health Optimization at Scale

QPN further supports population-scale behavior-shaping functions that adapt to environmental, behavioral, social, and economic contexts. Within each PPN, QPCs maintain a continuously updated model of an individual's health-determinant landscape, derived from encrypted lifestyle-signal trajectories, behavioral engagement patterns, environmental exposures, financial micro-stressors, and authenticated caregiver interactions. Because all processing occurs inside QPCs, the network can detect risk-relevant patterns—such as increasing sedentary behavior, nutritional instability, rising stress loads, deteriorating sleep cycles, or social withdrawal—without exposing any sensitive information to any external entity.

QPN can then generate environment-appropriate interventions by interacting in zero-knowledge form with the digital ecosystems the user already engages with. These interventions may include personalized defaults, dynamic filtering of harmful content, context-aligned incentive structures, risk-adaptive routing of recommendations, or micro-interventions triggered by clinically relevant changes in behavioral or physiological signals. All such interventions adhere to multi-party Trust Criteria and can incorporate clinician-defined constraints, employer-defined wellness rules, guardian controls, or public-health safety thresholds.

Because these behavior-shaping workflows operate atop the existing infrastructure of consumer online services, e-commerce platforms, financial apps, transportation tools, workplace systems, and device ecosystems, they can scale to national and global populations without requiring new integrations, new data exchanges, or new institutional agreements. The QPN's dual-use architecture ensures that these interventions occur with zero marginal cost, while maintaining full compliance with privacy, bias-prevention, employment-law, and health-equity constraints.

Examples include:

- Prioritizing healthier food options in search results and menus
- Providing EasyAccess incentives for nutritious meals or physical activity
- Guiding high-risk patients toward safer entertainment or social-media use
- Offering financial-wellness and stress-reduction nudges linked to clinical risk
- Integrating family or caregiver support into daily-life workflows
- Delivering micro-interventions when device telemetry suggests deteriorating stability
- Embedding prevention incentives into retail, transportation, and digital-service ecosystems

These effects are not driven by traditional medical workflows—they emerge automatically as a byproduct of QPN's participation in the broader economy. Every digital interaction

becomes an opportunity to reinforce healthy behaviors, detect early warnings, reduce risk exposure, and align incentives, without any additional cost, friction, or data sharing.

These capabilities stand in stark contrast to the limitations of today's healthcare system. Payers and providers—even with access to clinical records—cannot see the day-to-day environments that shape people's choices, cannot influence behavior at the moment decisions are made, and cannot integrate lifestyle, stress, social context, or environmental signals into clinical pathways. The Quantum Privacy Network gives them that capability *without* expanding surveillance, collecting new data, or breaching privacy. Instead, it provides a patient-controlled, zero-knowledge mechanism for interacting with the same digital ecosystems that already influence everyday life.

And the greatest beneficiary is the patient. Most people want better health, more energy, less stress, deeper sleep, more emotional stability, and fewer crises—not because an employer, payer, or clinician wants it, but because *they* want to feel well and live better. QPN simply reinforces the healthy defaults they already prefer, unobtrusively and automatically, through the digital choices they make every day. No one has to force this on anyone; healthier pathways become the easier, more convenient, more affordable options. Patients receive better outcomes with less effort. Clinicians gain more stable and supported patients. Employers see healthier, more resilient workforces. And society benefits from fewer avoidable crises and less chronic strain.

By making the healthy path the easy path—and doing so in a fully private, user-controlled way—the QPN turns everyday digital life into a continuous, person-centered support system. The result is empowerment, not control; agency, not surveillance; and a world in which improved health emerges naturally from the way people already live, work, move, eat, shop, and connect.

Employers, educators, and public agencies have strong reasons to support this transformation. Healthy, emotionally stable, well-supported employees and citizens are more productive, more engaged, and more likely to stay in their roles. Because the QPN's behavior-shaping capabilities operate with zero marginal cost, employers and institutions can subsidize or reinforce these benefits for their own reasons, reducing pressure on healthcare spending while improving population well-being.

As adoption spreads across consumer online markets, workplaces, e-commerce platforms, financial apps, and community services, QPN becomes ubiquitous—naturally pulling in the data needed to support personalized healthcare, while simultaneously exporting health-promoting intelligence back into the environments that shape behavior. This creates a self-funding, continuously learning societal infrastructure in which health,

productivity, and well-being are not separate goals, but emergent properties of the same privacy-preserving, AI-optimized network.

## A Nationwide Market for Better Health Value

Together, these self-funding dynamics and behavior-shaping capabilities create a new kind of national marketplace—one in which healthier outcomes are not merely hoped for but structurally incentivized. As QPN becomes embedded across the digital and physical environments people interact with every day, the network aligns incentives around prevention, long-term value, and sustained well-being.

Instead of the current system—where value is extracted from fragmentation, delays, and avoidable disease—the QPN marketplace rewards stakeholders for keeping people healthy, engaged, productive, and supported.

Patients and families benefit from healthier defaults and personalized guidance woven invisibly into the flow of daily life. Clinicians gain a real-time understanding of the factors influencing their patients' outcomes—without ever accessing raw behavioral or lifestyle data. Employers gain a healthier, more stable workforce with fewer avoidable absences and lower benefits spending. Communities benefit from reduced strain on social services, improved safety nets, and earlier detection of emerging risks. And the healthcare system benefits from a dramatic reduction in unnecessary utilization, administrative waste, and preventable deterioration.

Crucially, QPN and the Privacy Network Exchange do not impose this transformation through disruptive mandates, expensive platform replacements, or centralizing data into new silos. Instead, they leverage organic adoption, dual-use infrastructure, and market competition—allowing each participant to contribute data, intelligence, and workflows under conditions that remain fully private, fully compliant, and fully under user control.

By replacing fragmentation with continuity, friction with automation, and misaligned incentives with transparent, patient-centered value, the QPN marketplace becomes a self-reinforcing engine of national health improvement. Better choices become easier. Better care becomes more coordinated. Better outcomes become more predictable. And as the system scales, it becomes not only more efficient—but fundamentally more humane.

# 7.0 Direct-to-Patient, Direct-to-Consumer & Direct-to-Employer Contracting

For decades, pharmaceutical manufacturers, medical device companies, digital therapeutics vendors, and even employers have explored contracting directly with patients. Nearly half of the value of every prescription or specialty therapy is absorbed by intermediaries—PBMs, wholesalers, GPOs, distribution hubs, claims processors, and

retail pharmacies—before the product reaches the patient. These entities control pricing, benefits, eligibility checks, routing, formulary placement, and claims flows. They aggressively protect these positions through exclusive contracts, opaque data practices, and infrastructure lock-in. As a result, true direct-to-patient or direct-to-employer contracting has been structurally impossible at scale.

The Quantum Privacy Network (QPN) fundamentally rewrites these constraints. QPN creates a neutral, privacy-preserving computational substrate in which pricing, eligibility, benefits, logistics, payment, routing, and compliance workflows can occur without exposing PHI, triggering surveillance mechanisms, or requiring use of the rails controlled by PBMs, payers, or clearinghouses. Instead of building parallel infrastructures, manufacturers and employers rely on QPN's cryptographically governed execution cleanrooms for direct market access.

QPN enables lawful rights-holders—patients, clinicians, providers, employers, and government agencies—to automatically enforce their data rights. Each participant can contribute their own data into the patient's Personal Privacy Network (PPN). This reverses the traditional power dynamic: incumbents' data silos no longer constitute barriers to innovation. Patients and clinicians can include claims histories and medical records; employers can contribute coverage and benefits details. QPN reconstructs a complete, privacy-preserving evidence graph—one richer than any single incumbent can assemble, and one that no intermediary can block or detect.

## Dual-Use Access to Incumbent Infrastructure that can't be detected or blocked

Patients and clinicians already have accounts, credentials, and legal rights inside payer portals, PBM systems, provider networks, pharmacies, and diagnostic labs. QPN uses these as 'dual-use' infrastructure: it exercises existing rights on behalf of the patient inside a privacy-preserving workflow without altering the incumbent system. To the intermediary, each request appears as a routine member or clinician query. Within QPN, however, these interactions become part of a cryptographically constrained cross-organizational pricing, care, or contracting workflow—one that incumbents cannot detect, discriminate against, or block.

Direct-to-patient contracting requires payment rails that cannot be intercepted or penalized by PBMs. QPN supports this through private, unobservable financial instruments including single-use virtual debit tokens, EasyAccess Coupons, and privacy-preserving payment threads. These operate entirely within QPN-bounded workflow containers. They never produce NCPDP claims or payer-facing financial artifacts. PBMs cannot detect these transactions, apply accumulator rules, deny benefits, or retaliate. Manufacturers,

employers, or charitable organizations can directly fund patient affordability, with patients receiving full benefit without negative downstream consequences.

### EasyAccess Coupons as Programmable, Privacy-Preserving Reimbursement

EasyAccess Coupons extend QPN payment capabilities through a universal mechanism for delivering discounts, reimbursements, subsidies, and benefits. They work across point-of-sale systems, telehealth platforms, mobile devices, and e-commerce flows. They interoperate with the 8112 Universal Digital Coupon standard from The Coupon Bureau (TCB) and the legacy 8110 barcode standard. The 8112 standard provides serialized, real-time validation. QPN augments this with zero-knowledge eligibility, privacy-preserving personalization, role-based authorization (e.g., clinician, parent, or guardian approval), and cryptographic compliance enforcement. Inside QPN, these coupons become programmable healthcare affordability tools.

### Replacing Rent-Seeking Intermediaries with Patient-Centered Market Efficiency

QPN makes direct contracting structurally unstoppable. Workflows occur within cryptographically governed execution environments that incumbents cannot monitor, block, penalize, or exploit. PBMs cannot detect pricing logic; payers cannot prevent patient-controlled data contribution; wholesalers cannot intercept logistics flows. For the first time, manufacturers, employers, and patients can engage transparently, fairly, and privately, without imposing new infrastructure burdens or violating regulatory obligations.

The cumulative effect is transformative: QPN eliminates every chokepoint historically used to suppress transparency and extract economic rents. It shifts control of data from institutions to individuals. It allows neutral, private orchestration of benefits, payments, logistics, and clinical workflows. It enables a competitive, patient-centered health marketplace where value replaces friction, transparency replaces opacity, and patients regain control over both their data and their healthcare choices.

## 8.0 Value-Based Personalized Plan Design

For decades, health insurance plans have been built around rigid, population-level benefit structures. Regardless of clinical context, financial circumstances, disease severity, or personal goals, every member is forced into the same co-pays, deductibles, prior authorization rules, step-therapy requirements, and cost-sharing formulas. These one-size-fits-all designs were created for an era when payers had neither the technical means nor the legal ability to tailor benefits to individual patients in real time. As a result, plan

design has become one of the most powerful—and least adaptive—forces shaping healthcare decisions in the United States.

The gap between what modern healthcare *could* achieve and what current plans *allow* has grown enormous. Personalized care pathways, evidence-based treatment selection, real-time benefit optimization, and patient-centered economic incentives are all widely recognized as essential for improving outcomes and reducing costs. Yet none of these can be implemented reliably across today's fragmented infrastructure, where clinical data lives in EHRs, benefits data in payer systems, pharmacy data in PBMs, financial exposure in claims engines, and behavioral or social determinants data in entirely different ecosystems.

In such an environment, benefit personalization is impossible—not because the rules don't exist, but because the underlying infrastructure cannot safely compute across the necessary data.

The Quantum Privacy Network (QPN) resolves this long-standing structural limitation. It enables a new class of **dynamic, personalized plan designs** that adapt in real time to each patient's clinical conditions, lifestyle factors, benefit eligibility, financial exposure, and evidence-based care options—while keeping all sensitive data within cryptographically protected Privacy Domains. QPN allows computation, not data, to move across the ecosystem. This eliminates the need to centralize information or expose it to entities that lack the right to see it.

Under this model, a patient's Personal Privacy Network (PPN) becomes the home for a unified, fully privacy-preserving evidence graph. Clinical history, laboratory results, imaging, genomics, pharmacy data, plan rules, accumulators, social determinants, provider performance, behavioral patterns, and even digital therapeutic engagement can all be incorporated—without being revealed to payers, PBMs, clinicians, or manufacturers unless their legal rights explicitly permit it. QPN's cryptographically governed execution ensures that every stakeholder can contribute data they have the legal right to share, while the system respects and enforces every applicable regulatory constraint.

With this foundation in place, benefit structures can finally become adaptive. For any clinical decision—choosing a medication, selecting a provider, scheduling a diagnostic study, or evaluating treatment pathways—QPN can compute personalized cost, risk, and benefit information in real time, without contacting or modifying any payer backend. Co-pays may be reduced or waived for high-value, evidence-supported treatments. Deductibles may be adjusted downward for preventive care, digital engagement, or optimal provider selection. Out-of-pocket estimates can be calculated instantly, even when they depend on complex interactions between accumulators, prior authorization

requirements, preferred pharmacy networks, or manufacturer-funded affordability programs.

In this environment, patients are no longer making healthcare decisions blindly or reactively. They see the true cost of each option before they choose. Clinicians gain immediate visibility into patient-specific financial exposure and can help guide decisions without waiting for payer approvals or navigating multiple portals. And payers can encourage high-value care through dynamic incentives, without modifying their legacy claims engines or exposing member data.

This approach also solves a fundamental economic problem in U.S. healthcare: incentives have historically rewarded volume, not value. Providers are reimbursed the same regardless of whether the care was clinically optimal. Patients often pay more for high-value therapies than for low-value substitutes. Employers and public payers bear the long-term costs of unmanaged chronic conditions, while short-term decision-makers face no accountability. By enabling personalized benefit adjustments tied to evidence, risk, and projected outcomes, QPN realigns the entire ecosystem around value.

Equally important, QPN is the only platform capable of delivering this kind of personalization at a national or global scale. Traditional systems—EHRs, HIEs, PBM engines, payer portals, consumer apps, cloud data lakes, and FHIR-based APIs—cannot compute across multi-party PHI without violating privacy laws or requiring data pooling. They cannot incorporate multi-stakeholder rights, cross-jurisdictional constraints, or dynamic evidence updates into real-time benefit determination. And they cannot integrate clinical, financial, behavioral, and population-level factors into a single decision without creating unacceptable regulatory, operational, or security risks.

QPN solves these problems simultaneously. It enables real-time, privacy-preserving adjudication that evaluates all relevant factors inside cryptographically bounded computation environments. It enforces policy constraints through Trust Criteria and Proof-of-Trust verification. It orchestrates cross-organizational workflows through EasyAccess Threads that require no new integrations and cannot be blocked by intermediaries. And it empowers patients, clinicians, and authorized stakeholders to contribute their lawful data into the patient's PPN, giving personalized plan design access to the most complete evidence graph in the healthcare system.

The result is a transformation in how insurance benefits function—not as static, population-level structures, but as dynamic, adaptive, individualized mechanisms that support better choices, better outcomes, and lower total cost of care. Personalized plan design becomes a natural extension of QPN's larger mission: to create a unified, privacy-preserving, AI-optimized marketplace for health value, where incentives finally align with

outcomes and where every participant benefits from a system designed to work for people, not intermediaries.

## 9.0 Real-Time Adjudication & Consumer-Driven Health

For most patients in the United States, healthcare is a blindfolded experience. They rarely know in advance what a procedure, test, medication, or specialist visit will cost. They do not know how their choices will affect deductibles, accumulators, or out-of-pocket exposure. They cannot compare the value, quality, or long-term cost implications of different providers or treatment pathways. Even clinicians—who often want to help guide sensible financial decisions—lack the tools and visibility to do so.

This opacity is a structural feature of the existing system, not an accident. Every benefit determination relies on a patchwork of payer rules, PBM formularies, accumulator logic, prior-authorization criteria, network arrangements, provider contracts, and manufacturer affordability programs. These rules are distributed across siloed infrastructures that cannot compute together without revealing PHI, violating privacy laws, or conflicting with contractual and regulatory barriers.

The result is that **real-time adjudication—computing the true cost, coverage, and financial impact of a care option at the moment of decision—has never been possible at national scale.**

Patients are left guessing. Clinicians remain in the dark. Payers continue to rely on retrospective control mechanisms like denials, audits, and utilization management. And the healthcare economy remains one where informed consumer choice is structurally impossible.

The Quantum Privacy Network (QPN) resolves this limitation by enabling **real-time, privacy-preserving adjudication** for every stakeholder, at the moment decisions are made. Instead of routing benefit requests through legacy payer systems, QPN performs adjudication inside cryptographically protected Privacy Domains that unify the necessary evidence from all relevant data sources: clinical history, benefit eligibility, accumulator status, formulary logic, prior authorization rules, cost-effectiveness evidence, provider quality indicators, and patient-specific risk factors. These computations occur without exposing data to any unauthorized party—and without requiring payers, PBMs, pharmacies, or providers to modify their existing infrastructure.

This shift is transformative. For the first time, patients can understand precisely what a treatment will cost them before choosing it. They can see how different options affect deductibles, out-of-pocket spending, or long-term costs. They can compare clinicians and facilities not only on clinical quality, but on real-time cost-to-them and expected value.

They can understand whether a medication is fully covered, partially covered, blocked by step-therapy requirements, eligible for manufacturer co-pay assistance, or best purchased through a direct-to-patient channel.

Clinicians, likewise, gain clarity they have never had before. At the point of prescribing or referring, a clinician can see the patient's real-time financial exposure and personalized benefit structure. They can choose high-value providers that minimize out-of-pocket cost. They can adjust diagnostic or therapeutic choices based on evidence-supported cost-effectiveness. They can avoid initiating care that will later be denied by a payer, sparing both patient hardship and administrative burden.

Payers benefit as well. Instead of relying on blunt tools like denials, preauthorization backlogs, or retrospective utilization review, they can influence behavior through **transparent, dynamic incentives** that work in real time. Preventive care can have lower or zero cost-sharing. High-value prescriptions can be incentivized. Low-value testing, duplicative imaging, or inefficient site-of-care choices can carry higher cost-sharing signals. Because QPN enforces incentive logic inside privacy domains, these adjustments do not require modifying payer claims engines or exposing PHI to manufacturers or clinicians.

This real-time adjudication capability is not merely an operational improvement—it is the foundation for **true consumer-driven healthcare**. When patients have clear, immediate visibility into the real cost, value, and implications of their decisions, behavior changes. People choose higher-value providers. They select more effective and less risky treatment pathways. They avoid unnecessary procedures. They adhere more consistently to treatment plans, especially when financial incentives reinforce doing so.

Every major economic analysis of consumer behavior in healthcare has concluded the same thing: **transparency, when paired with personalized financial incentives, reduces cost and improves outcomes.** Yet transparency has never been achievable because adjudication required exposing sensitive financial and clinical information to multiple intermediaries. QPN eliminates this barrier by computing everything privately, with zero knowledge, and delivering only the necessary decision outputs to the patient and their care team.

QPN also enables this adjudication to operate across domains that have historically been incompatible. The same infrastructure can compute not only clinical benefits and medical coverage, but also pharmacy benefits, direct-to-patient pricing, manufacturer affordability support, digital therapeutic eligibility, wellness incentives, care management rewards, community-based service support, and even personalized behavioral or lifestyle benefits.

In every case, QPN ensures that sensitive data remains protected and that no stakeholder gains inappropriate visibility or control.

Perhaps most importantly, real-time adjudication becomes a way to **liberate the healthcare economy from the opaque pricing mechanisms** that have prevented competition for decades. When patients and clinicians can see the true cost and value of different options, providers are forced to compete on efficiency and outcomes rather than billing complexity. PBMs lose their ability to distort formularies for profit. Payers can shift from denial-based cost control to incentive-based value optimization. And manufacturers can participate directly in affordability workflows without revealing strategic pricing or triggering PBM surveillance.

In short, real-time adjudication transforms healthcare into a functioning marketplace—one where decisions are informed, incentives are aligned, and value becomes the central driver of choice. This is not achievable with any existing infrastructure. It requires the privacy-preserving computation, cross-organizational workflow orchestration, and neutral trust fabric of QPN. With QPN, real-time consumer-driven health becomes not only possible, but inevitable.

## 10.0 Global Risk Pooling & Value Sharing

The economics of healthcare remain fundamentally misaligned because risk is fragmented. Each payer—commercial insurer, Medicaid plan, Medicare Advantage organization, employer, or union trust—manages its own silo of financial exposure. Each provider system is accountable only for its attributed patients. Each PBM manipulates drug spending inside its own benefit shell. Manufacturers negotiate rebates and discounts across disconnected formularies, each designed to optimize the intermediary's economics rather than the patient's outcomes.

This fragmentation produces predictable distortions. High-risk and medically complex patients become financial liabilities rather than individuals deserving coordinated care. Preventive and early-detection services—especially those whose benefits accrue over long time horizons—are chronically underfunded because many patients churn between payers. Innovative therapies that reduce lifetime cost are often rejected because no single payer captures the long-term gains. Employers bear the brunt of rising premiums without any mechanism to influence the drivers of risk in the broader ecosystem.

Attempts to correct these distortions—such as value-based contracting or outcome-based reimbursement—have repeatedly failed because no existing infrastructure can compute

shared value, track multi-party attribution, or enforce cross-stakeholder obligations without exposing sensitive data or violating privacy regulations.

The Quantum Privacy Network (QPN) resolves these systemic failures by enabling **global, privacy-preserving risk pooling and value sharing** across all stakeholders in the healthcare ecosystem. For the first time, populations can be treated as unified cohorts rather than as disconnected payer-specific segments. High-risk individuals can be supported through shared funding mechanisms. Value generated through early intervention, evidence-based care, or improved adherence can be distributed proportionally across all parties who contributed to achieving it.

At the core of this capability is QPN's ability to construct **patient-centered, multi-party evidence graphs** that integrate clinical outcomes, cost trajectories, social determinants, behavioral factors, engagement patterns, and real-world evidence from across the ecosystem—without ever revealing data to unauthorized parties. Computation occurs inside Privacy Domains and Quantum Privacy Cells, allowing sensitive data from payers, provider systems, employers, manufacturers, and public-sector agencies to be combined and analyzed without ever being pooled or exposed.

This creates, for the first time, a **universally accessible actuarial substrate** capable of calculating shared risk and shared value at the individual and population level. Each stakeholder's rights, obligations, contributions, and upside are defined through cryptographically verifiable Trust Criteria. Population-level risk pools can be dynamically recomputed in response to changing demographics, social and environmental conditions, new therapeutic innovations, or emerging population health threats. Attribution logic—historically one of the most contentious elements of value-based care—can be computed transparently and privately, with full auditability via immutable Trust Blocks.

Under this model, global risk pooling becomes both operationally feasible and economically rational. Cost savings achieved through reduced hospitalizations, optimized medication pathways, better chronic disease management, or preventive interventions can be shared across all stakeholders who contributed to those outcomes. High-risk populations—including individuals with chronic diseases, rare conditions, behavioral health challenges, or multi-system dependencies—can be supported through pooled funding mechanisms that reflect the true social value of maintaining health, independence, and productivity.

This structure also eliminates one of the most damaging economic distortions in American healthcare: the misalignment between **who pays** and **who benefits**. Today, commercial plans often refuse to invest in preventive care or long-term interventions because patients

churn every 12–36 months. Public-sector systems bear the downstream cost of untreated or poorly managed conditions. Manufacturers struggle to secure coverage for curative therapies because no payer wants to shoulder the upfront cost when the long-term savings accrue to someone else.

Global risk pooling allows these long-term gains to be distributed across the full population-level value chain. Employers may fund early-detection benefits that reduce long-term public expenditures. Medicaid agencies may benefit from employer-supported chronic disease programs. Commercial payers may receive shared savings from curative or gene-based therapies even when members transition into other plans. And manufacturers can structure outcome-based agreements where financial exposure and reward are shared among all parties in proportion to their contributions to value creation.

Crucially, QPN ensures that this system cannot be manipulated or blocked by entrenched intermediaries. Because computation occurs within privacy-preserving execution environments, no stakeholder can interfere with attribution, suppress evidence, alter outcomes reporting, or distort pooling algorithms for financial gain. Trust Blocks record every attribution event, value-distribution calculation, and compliance check, creating a transparent and auditable foundation for multi-decade population health contracts.

The societal implications are profound. A unified risk pool creates incentives for early intervention, preventive care, healthy behaviors, and long-term investment in population health infrastructure. Provider systems are rewarded for improving outcomes rather than maximizing billable volume. Employers benefit from a healthier and more productive workforce. Public-sector agencies see reduced long-term expenditures. And patients—especially those with chronic or complex conditions—benefit from a system that finally aligns around their long-term well-being rather than short-term cost containment.

QPN turns risk pooling from an actuarial abstraction into a living, adaptive, cryptographically enforced marketplace for shared value. It allows the healthcare system to behave as a coordinated network, where resources flow to where they generate the greatest benefit, and where every participant has a stake in improving population health.

In doing so, QPN establishes the foundation for a truly sustainable, efficient, and equitable healthcare economy—one where incentives reinforce, rather than undermine, the collective pursuit of better outcomes at lower cost.

## 11.0 Personalized Portable Reinsurance & the Economics of Long-Term Health

**One of the most persistent structural failures in the U.S. healthcare system arises from the way financial risk is assigned, transferred, and managed.** Health risk does not

follow payer boundaries, benefit-year cycles, employment status, or insurance plan transitions—yet the financing mechanisms for covering medical risk treat these boundaries as if they were natural divisions. Individuals routinely change insurers every 12 to 36 months due to job changes, plan transitions, geographic mobility, or movement between commercial and public programs, but these transitions break the continuity of financial responsibility that long-term health improvement requires.

This churn creates a profound misalignment: the entities best positioned to invest in long-term health are rarely the ones who capture the long-term benefits**. Commercial insurers hesitate to fund early detection, preventive care, metabolic reversal, mental-health stabilization, or curative therapies because the value unfolds over years and is likely to benefit a different payer.** Employers face the same challenge, often hesitating to invest in behavioral interventions or high-cost therapies when employees frequently move on. Public-sector payers inherit the downstream consequences of delayed diagnosis and unmanaged chronic disease but lack the leverage to influence upstream investment decisions made in the commercial sector.

Catastrophic, progressive, or chronic conditions—late-detected cancer, metabolic diseases, rare disorders, inherited conditions, and diseases requiring expansive long-term management—expose this misalignment most acutely. Early, decisive interventions can dramatically alter lifetime cost and outcomes, yet the payer who would need to finance the intervention is rarely the one who benefits from the improvement.

**Traditional insurance tools—reinsurance, stop-loss, risk adjustment, carve-outs—have repeatedly failed to fix this because they operate at the plan or employer level rather than at the individual level.** They cannot follow patients across insurers, providers, or employers; cannot track multi-year outcomes; cannot enforce long-term cost-sharing rules; and cannot attribute value across stakeholders without exposing sensitive PHI or centralizing data. The result is a system structurally biased against early investment and structurally favorable toward short-term financial gaming.

The Quantum Privacy Network (QPN) enables a breakthrough solution: **personalized portable reinsurance**, a patient-centered, cryptographically governed mechanism for linking risk coverage to the individual rather than to the payer. Instead of being embedded inside a single insurance product or employer arrangement, reinsurance contracts exist as privacy-preserving digital instruments anchored within the patient's Personal Privacy Network (PPN). **These instruments move with the patient, preserving continuity of coverage, attribution, and financial responsibility across insurers, employers, benefit years, geographic regions, and care settings.**

## The Structural Failure of Legacy Risk Models

Legacy risk models collapse under three constraints:

1. **They are tied to institutions rather than to people.**
2. **They depend on retrospective claims rather than real-time signals.**
3. **They cannot follow individuals across payer boundaries.**

A payer may see extensive fragments of a patient's historical data, but the data is often stale, incomplete, error-prone, and stripped of the behavioral and lifestyle context that drives cost and outcomes. Employers see only benefits usage. PBMs see pharmacy but not clinical history. Public health agencies see delayed and incomplete signals. Researchers see de-identified, retrospective information that cannot power real-time value-based contracting. Because each party sees only a snapshot of the patient through its own distorted lens, no party has the full picture needed for proactive risk management.

And because these snapshots are institution-bound, contracts cannot follow patients. Value cannot be fairly attributed. No payer has a durable incentive to act early. The result is widespread underinvestment in prevention, early detection, metabolic stabilization, mental-health maintenance, and high-value therapies.

## QPN's Breakthrough: Patient-Anchored Risk Coverage

The Quantum Privacy Network reverses the logic of risk by anchoring coverage in the patient, not the payer. Reinsurance contracts, value-sharing rules, cost offsets, and long-term obligations exist as digital instruments in the patient's PPN, enforced by cryptography rather than by institutional boundaries.

When a payer or employer funds an early intervention—such as preventive screening, metabolic reversal, behavioral stabilization, or a curative therapy—QPN generates an immutable attribution record documenting who funded the intervention, when it occurred, and what population-level downstream costs were actuarially avoided. These attribution records are bound to clinical outcomes, behavioral trajectories, and risk signals computed inside QPCs. They can persist for years or decades without ever exposing PHI to any stakeholder.

Because these attribution blocks are patient-anchored, they travel with the patient. If the patient changes insurers, employers, or public programs, the new payer inherits the patient's improved risk profile and automatically assumes its share of the value-sharing obligation. The system ensures that financial responsibility and financial benefit follow the same path: the patient's actual health trajectory.

## Guaranteed Value Sharing Across Future Payers

Personalized portable reinsurance allows each intervention to carry its value across time. Future payers inherit the improved risk profile and repay the fraction of avoided downstream cost owed to the earlier payer who created the value. Settlement is performed through privacy-preserving multi-sponsor workflows inside QPCs. Because settlement occurs through cryptographic execution rather than claims intermediaries:

- **no payer can block payment**
- **no entity can gather sensitive patient information**
- **no one can tamper with attribution**
- **no misaligned party can distort outcomes**

This makes long-term health investment not only possible but provably profitable.

## Patient-Centered Global Reinsurance Pools

QPN enables the creation of global reinsurance pools organized around the patient rather than the institution. These pools operate using encrypted, high-resolution lifestyle and behavioral signals generated inside PPNs—signals that no other stakeholder can access, reproduce, or infer.

Reinsurers gain precision analytics based on stress patterns, metabolic stability, sleep cycles, nutritional exposure, medication adherence, environmental triggers, engagement stability, and caregiver interactions. Because QPCs compute risk internally, reinsurers receive actionable risk markers without ever receiving raw data.

The result is the first closed-loop reinsurance system where reinsurers can measure risk, influence behavior, evaluate outcomes, and reward value creation in real time without violating privacy.

## Why Payers Will Need to Participate

Participation becomes inevitable because non-participation becomes economically self-defeating, if not suicidal.

A payer that opts out of the reinsurance ecosystem cannot measure or manage risk with any meaningful accuracy, because it lacks access to the patient's global privacy graph—the only environment where lifestyle trajectories, engagement stability, early-warning signals, environmental exposures, medication-adherence patterns, caregiver interactions, and other behavioral determinants are continuously analyzed. None of this information exists in claims, EMRs, PBM feeds, wellness apps, or any other legacy system.

Without these signals, an outside payer is effectively operating blind: its underwriting becomes less precise, its care management less effective, its incentives misaligned, its routing inferior, and its cost structure permanently higher.

Moreover, PPNs will naturally route unmanaged or uncovered utilization to non-participating payers because the reinsurance ecosystem cannot safely distribute risk to entities that refuse to join. This is not a punitive tactic, nor can it be blocked by the payer; it is simply the financially rational choice for the patient and the unavoidable operational consequence of opting out of a shared risk framework that governs both data access and care workflows. When a payer declines to participate, the system has no mechanism to allocate costs elsewhere—so those costs inevitably accrue to the payer standing outside the network.

Conversely, participating payers gain unprecedented predictive insight and risk-management capability. They gain access to the richest encrypted risk model ever assembled; the ability to influence behaviors that drive cost; and predictable, actuarially sound mechanisms for sharing long-term financial value. For insurers, these capabilities represent the kind of underwriting precision they have dreamed about for decades.

## Wall Street Will Underwrite This Market

With risk accurately measurable, influenceable, and transparently attributed, global investors—from reinsurers to sovereign funds to investment banks—will eagerly enter the market. They will create securitized instruments backed by the avoided downstream costs of preventive care, metabolic reversal, mental-health stabilization, and curative therapies.

Employers and payers will offload high-risk trajectories into global reinsurance pools, just as banks sell mortgages into secondary markets. This dramatically de-risks payer balance sheets and creates sustainable financing for prevention and early intervention.

**Because global reinsurance pools capture the full long-term value of improved health, they naturally become the primary purchasers of high-impact therapies**—gene therapies, metabolic reversal treatments, advanced digital therapeutics, early-detection technologies, and tools for mental-health stabilization. For the first time, researchers and pharmaceutical innovators can sell not just molecules, but long-horizon value, with guaranteed downstream payment tied directly to reductions in lifetime cost-of-disease. This model bypasses layers of intermediaries and administrative friction, **allowing pharmaceutical and device manufacturers to lower prices, expand access, and simultaneously increase profitability—because value is recognized, attributed, and monetized across the full arc of a patient's health trajectory.**

## A New Health Economy Emerges

With personalized portable reinsurance, prevention becomes profitable rather than expensive. Early detection becomes economically rational instead of financially punitive. Metabolic and mental-health stabilization become core risk-management strategies rather than soft benefits. Employers can reduce disability risk and offload long-term liabilities. Payers are finally rewarded for acting early. Manufacturers are paid for long-term

outcomes rather than process measures. Researchers gain guaranteed returns for innovations that reduce lifetime disease burden.

**And patients benefit most of all.** The system begins optimizing for what people actually want: better health, lower stress, more stability, and longer, healthier lives.

### The Architectural Pillars

Three mechanisms make this possible:

- **Patient-anchored evidence graphs** unify outcomes, utilization history, adherence, risk trajectories, value attribution, and financial exposure inside a cryptographically protected PPN.
- **Portable digital risk instruments** encode specific actuarial rules, triggers, obligations, and reimbursement pathways that follow the patient across time.
- **Cross-payer continuity and adjudication** ensures that contracts remain enforceable and operational across all payers and care settings, with each event recorded as an immutable Trust Block.

### The Result

The Quantum Privacy Network transforms reinsurance from a blunt, population-level financial tool into a precise, individualized, encrypted system for long-term value creation and equitable cost distribution.

It realigns incentives across the healthcare economy, sets the financial foundation for prevention and early intervention, and enables a sustainable high-value care ecosystem where every stakeholder benefits from improving long-term outcomes—and where the patient's well-being becomes the organizing principle of the entire risk economy.

## 12.0 Personalized Medication Therapy Management

Medication therapy is one of the most powerful drivers of health outcomes—and one of the most failure-prone components of modern healthcare. More than half of all adverse events, hospital readmissions, chronic-disease escalations, and avoidable deaths are directly tied to medication mismanagement. Patients routinely receive duplicative therapies, contraindicated combinations, unsafe drug–drug or drug–disease pairings, incorrect dosages, and unnecessary treatments. Adherence failures—missed doses, unfilled prescriptions, early discontinuation, or unreported side effects—are pervasive. Clinicians lack visibility into medications prescribed by other providers, pharmacies rarely see the whole picture, and PBMs have no insight into clinical context.

The result is a system where **no one has a complete or trusted view of what a patient is actually taking**, what they should be taking, or what they can safely afford.

Traditional Medication Therapy Management (MTM) programs attempt to solve this through manual pharmacist consultations, payer-driven adherence programs, and EMR-integrated alerts. But these approaches fail at scale for three structural reasons:

1. **No entity has full access to the medication evidence graph:** Each participant sees only a partial and operationally constrained view: Even where data exchange exists, it is often stale, error-prone, incomplete, or distorted by mismatched formularies, missing context, or inconsistent coding. No existing architecture can unify these fragments into a complete, trustworthy, privacy-compliant medication graph without violating regulatory boundaries or exposing sensitive information.

2. **MTM requires computation across highly sensitive, regulated, and proprietary data**: Clinical histories, lab data, genomics, psychosocial factors, behavioral context, affordability, and household dynamics all influence safe medication use. No existing interoperability or claims architecture can compute across these sources in a privacy-preserving, cross-organizational manner.

3. **Medication optimization is a longitudinal, multi-stakeholder workflow:** Safe and effective therapy management requires:
    - ongoing pharmacist/clinician review
    - real-time detection of gaps or risks
    - adherence support
    - timely renewals
    - affordability optimization
    - coordination with caregivers
    - dynamic benefit recalculation
    - evidence-based e-consults at prescribing time

    Existing systems cannot orchestrate these workflows across organizations.

The Quantum Privacy Network (QPN) resolves these problems by providing the technological substrate required for safe, continuous, patient-centered medication management at national scale.

## Unified, Privacy-Preserving Medication Evidence Graphs

Within QPN, a patient's Personal Privacy Network (PPN) securely unifies data from clinicians, pharmacies, PBMs, payers, labs, behavioral health providers, device telemetry, and patient self-report—all without centralizing raw data or exposing PHI. QPN's cryptographically bounded execution allows:

- medication lists

- claims histories
- clinical notes
- lab values
- genomics
- social determinants
- cost and benefit data
- adherence signals
- adverse-event patterns

to be integrated into a **single computable evidence graph** while remaining isolated inside privacy domains. This creates, for the first time, a complete and trustworthy foundation for personalized therapy optimization.

## Continuous Personalized Medication Safety and Optimization

QPN enables real-time, dynamic medication safety evaluation that adjusts as the patient's context changes. Within Privacy Domains, AI agents and clinical rules engines can evaluate:

- contraindications and drug–drug interactions
- renal/hepatic dose adjustments
- duplicate therapy risks
- specialty-drug safety parameters
- genomic contraindications
- lifestyle or behavioral risk factors
- formulary alternatives and clinical appropriateness
- REMS or safety-protocol compliance
- potential overuse, underuse, or misuse

Because computation occurs in private execution environments, no party—clinician, PBM, pharmacy, payer, or vendor—needs to see data they are not legally entitled to access.

## Evidence-Based e-Consults at Prescribing and Renewal Time

QPN enables real-time clinical and affordability e-consults that present clinicians with personalized evidence:

- preferred evidence-based therapies
- cost-effective alternatives
- formulary-based recommendations
- affordability projections
- patient-specific risk alerts
- dynamic prior-authorization logic

- opportunities for digital therapeutics or care pathway enrollment

These consults run inside QPCs, so neither PBMs nor payers can detect when clinicians access more affordable options or manufacturer support programs. This prevents anti-competitive steering and protects clinician autonomy.

## Automated Care Coordination for Complex Therapies

For patients with chronic conditions, polypharmacy, or specialty medications, QPN orchestrates long-running medication-management threads involving:

- primary clinicians
- specialists
- pharmacists
- caregivers
- adherence coaches
- home-delivery networks
- manufacturers and patient-support hubs
- payers and employer sponsors

These interactions occur without the need for shared portals, shared EMR systems, or centralized PHI pooling. Each role operates within their own privacy domain with only the minimal rights required for safe coordination.

## Personalized Adherence Support and Behavioral Integration

QPN allows adherence logic to be dynamically personalized using contextual signals:

- device data
- symptom logs
- behavioral and lifestyle inputs
- risk-prediction AI models
- patient preferences
- affordability status
- family/caregiver involvement

Agents can provide nudges, educational prompts, side-effect monitoring, refill reminders, and care-plan adjustments—all inside the patient's PPN.

## Value-Based Reimbursement for Pharmacists, Clinicians, and Caregivers

QPN enables automated, privacy-preserving attribution of value to those who improve medication outcomes. Using Trust Blocks and PoT verification, the system can reward:

- pharmacists managing complex regimens

- clinicians resolving gaps in care
- caregivers supporting adherence
- digital therapeutics that improve safety or outcomes
- community health workers preventing escalation

Payments and incentives can be tied to actual improvements measured longitudinally across payers, providers, and benefit years—something no claims-based system can do today.

### Home Delivery, Automated Refills, and Personalized Logistics

Within QPN-bounded workflow threads, medication fulfillment can include:

- home delivery with privacy-preserving authorization
- dynamic refill scheduling
- automated prior auth renewals
- manufacturer-support program integration
- "invisible" affordability assistance that avoids PBM retaliation

Because PBMs cannot detect these workflows, they cannot interfere with manufacturer support, direct fulfillment, or value-based pricing arrangements.

## 13.0 Personalized Therapy Warranties & Outcomes-Based Contracts

The emergence of high-cost cell and gene therapies, curative biologics, specialty medications, and precision therapeutics has exposed a structural barrier in U.S. healthcare: **payers bear financial risk immediately, while clinical value is realized over years or decades**. As a result, many life-changing therapies are denied or delayed, not because they lack clinical merit, but because **no existing infrastructure allows payers and manufacturers to share risk, measure outcomes, or reconcile value over time**.

To address these failures, manufacturers have attempted performance-based agreements—often referred to as therapy warranties, outcomes-based contracts, or value-based pricing arrangements. But these efforts remain rare, fragile, and limited to small pilots. The underlying reason is simple: **no existing system can monitor outcomes, enforce warranties, or reconcile financial obligations in a privacy-preserving, cross-payer, cross-provider environment.**

The Quantum Privacy Network (QPN) introduces the technical, legal, and operational infrastructure necessary to make personalized therapy warranties practical, compliant, scalable, and economically sustainable at a national scale.

## The Structural Failure of Existing Approaches

Today's infrastructure cannot support outcomes-based therapy contracts because:

- **No participant has access to the full longitudinal outcome data** needed to assess whether a therapy "worked"—data is distributed across EMRs, labs, claims systems, and patient devices.
- **Cross-payer continuity is impossible**—if a patient switches plans, the original payer never benefits from long-term outcomes.
- **Manufacturers cannot safely or legally access PHI**, eliminating their ability to validate performance or facilitate care management and adherence.
- **Payers cannot monitor adherence or dosing behavior** without intruding on patient privacy.
- **Regulatory constraints prohibit most multi-party data sharing** required to administer warranties.
- **The claims system is incapable of measuring clinical outcomes**—only transactions.

As a result, current therapy warranties either collapse under their own data requirements or require massive manual work, legal complexity, or bespoke integrations that cannot scale. **QPN resolves all of these foundational limitations.**

## QPN Administration of Personalized Warranties

QPN enables privacy-preserving, longitudinal evidence graphs that can safely unify:

- clinical outcomes and lab results
- imaging and diagnostics
- symptom logs and PROs
- medication adherence and dosing behavior
- hospitalization events
- real-world evidence (RWE)
- claims and utilization data
- genomic or biomarker status
- social and behavioral attributes
- care-plan milestones

**Computation occurs inside QPC-bounded Privacy Domains**, meaning that outcome evaluation:

- never exposes PHI,
- never centralizes raw data,
- never violates HIPAA or 42 CFR Part 2,

- and never grants direct access to manufacturers.

Stakeholders contribute their portions of the data—clinicians, labs, pharmacies, payers, and patients themselves—without revealing sensitive details. The QPN computes warranty eligibility, outcome achievement, dosing adequacy, adherence sufficiency, and relapse events through zero-knowledge analytics and verifiable workflow execution.

## Personalized, Patient-Specific Therapy Warranties

Within QPN, therapy warranties become patient-specific, adaptive, and automatically enforceable. Contracts can incorporate:

- individualized baseline risk
- biomarker-verified expected response
- genomic suitability
- disease-progression modeling
- anticipated outcomes over defined timeframes
- dynamic monitoring windows
- adherence-adjusted criteria
- cross-payer participation
- real-world evidence calibrations

This transforms warranties from blunt, population-average constructs into precision value-based agreements tailored to each patient.

## Cross-Payer Continuity and Portable Warranty Tracking

A historic problem in outcomes-based contracts is payer discontinuity. QPN solves this through **portable warranty threads** tied to the patient's PPN rather than to any institution. This allows:

- warranties to follow patients across commercial plans
- long-term outcomes to be monitored without payer-to-payer PHI exchange
- blended multi-payer funding models
- employer participation in outcomes evaluation
- regional or national value-sharing pools

**Manufacturers can stand behind their therapies confidently, knowing outcomes can be independently and securely assessed**—even if the patient changes health plans multiple times.

## Automated, Cryptographically Enforced Warranty Administration

**QPN enables fully automated warranty execution**:

- Clinicians, labs, pharmacies & devices contribute data via Trust-verified channels.

- QPN computes zero-knowledge outcome verification.
- If the therapy meets the expected result, the contract completes with no action needed.
- If the outcome fails, the warranty triggers a cryptographic enforcement of a payment or reimbursement.
- Trust Blocks record all underlying evidence and contractual compliance for auditability.

All of this occurs without exposing PHI to manufacturers or intermediaries.

## Shared Savings, Premium Stabilization, and Value Recycling

With QPN, therapy warranties can be integrated into broader economic structures:

- value-sharing across payers, employers, and public programs
- stabilization of premiums for high-cost therapies
- pooling of risk across populations
- reallocation of savings from effective therapies into coverage expansion
- integration into personalized plan design and affordability logic

This turns outcomes-based contracts from boutique pilot programs into **scalable mechanisms for financing innovation**.

## Benefits for Patients, Payers, Manufacturers & Society

QPN-enabled outcomes-based agreements deliver benefits impossible under traditional systems:

### For patients:

- faster access to life-changing therapies
- reduced out-of-pocket costs
- personalized affordability and risk protection
- higher trust and transparency
- improved long-term outcomes

### For payers and employers:

- reduced financial uncertainty
- protection against treatment failure
- alignment with long-term population outcomes
- portable risk contracts across plan years

### For manufacturers:

- faster uptake of innovative therapies

- reduced payer resistance
- ability to stand behind performance transparently
- better real-world evidence and post-market insights

### For society:

- improved longevity and productivity
- lower long-term healthcare spending
- accelerated innovation in curative therapies
- alignment of economic incentives with real patient benefit

### Conclusion

Personalized therapy warranties have long been recognized as an essential tool for financing high-cost, high-value therapies. But until now, no technical, legal, or operational infrastructure existed to make them viable at scale. The Quantum Privacy Network provides that infrastructure.

By unifying evidence, enforcing privacy, orchestrating multi-party workflows, supporting cross-payer continuity, and enabling cryptographically verified outcome measurement, QPN transforms outcomes-based contracts from theoretical constructs into practical, automated, equitable financial instruments.

For the first time, the healthcare system gains the ability to pay for therapies based on actual patient outcomes—safely, privately, and at a national scale.

## 14.0 Consumer-Directed Health & Personalized Incentive Ecosystems

Consumer-driven healthcare has long promised to empower individuals with choice, price transparency, and control over their care. But in reality, U.S. healthcare has never delivered a true consumer-driven market. **Patients lack actionable price information, benefit structures are opaque, incentives are misaligned, and payers, PBMs, and intermediaries control and manipulate the systems that determine costs & coverage**.

Even when patients attempt to make informed choices, the infrastructure they rely on—patient portals, PBM apps, benefits tools—cannot provide real-time, personalized, evidence-based guidance.

**The Quantum Privacy Network (QPN) finally makes consumer-directed healthcare possible by enabling personalized, privacy-preserving, economically aligned incentive ecosystems** where patients, clinicians, employers, and payers can collaborate transparently and safely. QPN transforms static, one-size-fits-all benefit designs into

dynamic, individualized incentive systems that respond to each patient's health needs, preferences, risk factors, financial realities, and care-pathway context.

## Why Consumer-Directed Healthcare Has Failed Historically

Consumer choice in healthcare has failed due to structural barriers:

- **Patients do not know what care will cost:** Prices vary dramatically, but no system reveals patient-specific out-of-pocket expenses in real time.
- **Payers and PBMs obscure incentives:** Formularies, prior authorizations, step-therapy rules, accumulator programs, and benefit restrictions make true choice impossible.
- **Providers cannot guide patients based on price or coverage:** Clinicians rarely see patient-specific cost exposure or benefit design logic.
- **Affordability support is disconnected from care decisions:** PA approvals, co-pay maximizer logic, and pharmacy benefit rules undermine price transparency and affordability programs.
- **Incentives are misaligned:** Plans and providers often financially benefit from high utilization, unnecessary care, or misdirected treatment pathways.

Today's infrastructure cannot support consumer-directed health because it lacks:

- real-time patient-specific adjudication
- personalized benefit design
- cross-stakeholder coordination
- zero-knowledge privacy protection
- dynamic incentive adjustment
- unified multi-party workflow execution
- neutral governance

QPN provides these capabilities natively.

## Personalized Incentive Ecosystems Within Personal Privacy Networks

Inside a patient's Personal Privacy Network (PPN), QPN unifies clinical data, benefits, risk factors, outcomes, affordability information, behavioral drivers, and care histories into a **dynamic, evidence-based incentive engine**.

This enables real-time personalization of:

- co-pays
- deductibles
- provider steering
- digital therapeutic access
- preventive-care incentives

- medication-adherence rewards
- chronic-disease management incentives
- wellness and lifestyle adjustments
- plan-selection recommendations
- “value boosts” for high-impact care
- cost reductions when choosing better providers

These adjustments are computed **privately**, without exposing PHI to plans, PBMs, or vendors.

## Dynamic Real-Time Incentives at the Point of Decision

QPN allows incentives to adapt instantly to patient decisions:

- When a patient compares two providers, QPN can compute personalized co-pays based on quality and cost-effectiveness.
- When a clinician prescribes a medication, QPN can provide real-time, evidence-based, personalized formulary guidance.
- When a patient schedules an MRI, QPN can reduce the patient's out-of-pocket costs for choosing a higher-value facility.
- When preventive screenings are overdue, QPN can offer zero-cost or reward-based incentives.
- When chronic-disease risks escalate, QPN can adjust benefits to encourage early intervention.

These incentives appear **in the patient’s PPN**, not a payer portal, making them accessible, trusted, and frictionless.

## Incentive Alignment Across Patients, Payers, Providers, Manufacturers & Employers

The QPN supports *multi-stakeholder incentive funding*, enabling:

- employers to reward preventive care
- payers to reduce patient cost exposure
- clinicians to receive adherence incentives
- manufacturers to fund affordability and outcomes incentives
- public-sector agencies to subsidize specific interventions
- family members to contribute funds for lifestyle improvements

All flows occur inside privacy-preserving workflow threads with immutable Trust Blocks for transparency and compliance.

## Zero-Knowledge Pricing, Benefits, and Quality Comparisons

QPN enables real-time comparisons of:

- providers
- care pathways
- digital therapeutics
- pharmacies
- medications
- specialty-care options

using zero-knowledge metrics, meaning the patient sees personalized cost, quality, and outcome data without exposing their PHI and without any competitor accessing proprietary provider or payer data. The net result is that **patients receive clear, personalized decision guidance** without violating privacy or revealing sensitive contractual data among healthcare incumbents.

## Consumer-Driven Markets for Care, Benefits, and Outcomes

QPN transforms healthcare from a payer-centric model into a **consumer-driven marketplace** where:

- patients choose care based on transparent value
- clinicians compete on outcomes, not billing
- digital therapeutics integrate directly into care pathways
- pharmacies and delivery partners compete on convenience and safety
- manufacturers offer direct-to-patient incentives or benefits
- employers contribute to individual incentives aligned with productivity and health improvements
- public agencies support population health through targeted, privacy-preserving subsidies

The marketplace is **patient-centered**, not institution-centered.

## Integration with Personalized Plan Design and Global Risk Sharing

Sections 8 through 13 collectively establish the infrastructure needed for a fully aligned incentive ecosystem. **Personalized plan design** (Section 8) identifies the most clinically appropriate and cost-effective choices for each individual. **Real-time adjudication** (Section 9) brings transparency to actual prices, benefits, and cost exposures at the moment decisions are made. **Global risk pooling** (Section 10) aligns incentives across entire populations, making prevention and early detection financially rational for all participants. **Personalized portable reinsurance** (Section 11) extends that alignment across insurers, ensuring that upstream stakeholders share in downstream savings even when members change payers. **Medication Therapy Management** (Section 12) improves

safety, adherence, and clinical stability, while **Personalized Therapy Warranties** (Section 13) finally tie payment to verified real-world outcomes rather than transactional events.

Section 14—**Consumer-Directed Health & Personalized Incentive Ecosystems**—then completes the architecture. It provides the real-time, consumer-facing layer that unifies all of these components into a coherent experience in which individuals receive personalized incentives, early-warning signals, healthier defaults, and context-aware support. This final layer ensures that the economic logic, clinical evidence, safety systems, and risk-sharing mechanisms established in the prior sections work together seamlessly to guide daily choices, support better outcomes, and deliver a continuously improving healthcare experience.

### Outcomes: True Consumer Control for the First Time

QPN makes possible what the U.S. healthcare system has attempted—and failed—to deliver for 30 years:

- transparent, real-time, patient-specific pricing
- personalized cost-sharing aligned with value
- unbiased decision support
- competition among providers and payers based on value
- consumer-driven care navigation
- privacy-preserving benefits and incentive flows
- patient empowerment without institutional surveillance
- neutral, tamper-proof incentive alignment across the ecosystem

**Patients finally gain control over their care choices, their financial exposure, and their health outcomes—supported by a system that aligns incentives rather than obstructing them.**

## 15.0 Population Health Optimization & AI-Driven Preventive Care

### Persistent Failure of Population Health in the U.S.

For decades, the United States has tried and failed to build a learning, adaptive, population-level health system. Enormous resources have gone into risk-adjustment formulas, care-management programs, wellness campaigns, and public-health surveillance networks. Yet the system still behaves as if it were looking in a broken rear-view mirror: dashboards based on old claims, registries that update slowly, and reports based on dirty data that arrive months after the events they describe.

Data is scattered across EMRs, payers, PBMs, labs, pharmacies, employers, and government agencies. Each stakeholder sees only a narrow, institution-specific slice of a person's life. What they see is often stale by the time it arrives, shaped by the operational

context in which it was generated, and distorted by gaps, errors, incentives, and occasional fraud or manipulation.

Even when data is reasonably accurate, it is locked behind proprietary infrastructures, inconsistent standards, incompatible semantics, and business or regulatory constraints that prevent meaningful, patient-centered integration. Privacy laws—including HIPAA, 42 CFR Part 2, state privacy statutes, genetic-privacy restrictions, and emerging AI-governance rules—appropriately protect individuals, but also prevent enterprises from pooling sensitive data at scale, especially across institutional or jurisdictional boundaries. Interoperability challenges, uneven data quality, and misaligned incentives create blind spots and systematic biases that undermine both analytics and action.

Public-health agencies face the same fragmentation and delay. They rely on incomplete submissions and delayed reporting from thousands of independent sources with widely varying capabilities. Signals of emerging threats—behavioral-health deterioration, infectious-disease clusters, environmental-exposure impacts, medication-safety concerns, chronic-disease deterioration—often arrive too late, too noisy, or too fragmented to support effective preventive response.

## Quantum Privacy as the Missing Infrastructure Layer

The Quantum Privacy Network (QPN) is designed to change this without weakening privacy protections. Rather than trying to move or pool data, QPN makes it possible to compute across data wherever it resides, under cryptographic guarantees that nothing sensitive can leak.

Within QPN, all data is bound to Trust Criteria and Trust Credentials using immutable Trust Blocks that encode provenance, rights, obligations, and policy constraints. These constraints are automatically inherited by any aggregate, derivative, or downstream computation, creating a mathematically guaranteed chain of custodianship and accountability. All computation runs inside a decentralized mesh of Quantum Privacy Cells (QPCs) and Privacy Domains connected by Privacy Pipes, which allow information to be linked, pooled, partitioned, recombined, and repeatedly reprocessed with proofs that no sensitive information can be exposed to any person, organization, system, or device. There are no privileged insiders that you need to trust with the keys to your data.

Most data and outputs never need to be revealed in clear text; when disclosure is necessary, the EasyAccess Authorization Network enforces access at the finest possible granularity—down to a single attribute, for a specific purpose, on a particular device, for a strictly time-bound interval. By combining these layers, QPN eliminates the traditional tradeoff between privacy, personalization, and policy enforcement, allowing billions of Personal Privacy Networks and Enterprise Privacy Networks to safely support national-

scale public-health intelligence, patient safety, observational research, care delivery, and cross-sector population health.

Within this architecture, each person's clinical history, biometrics, lifestyle signals, environmental exposures, device telemetry, social determinants, benefit design, and engagement patterns can be analyzed in encrypted form inside QPCs. Population-level AI models receive only zero-knowledge outputs—structured signals that indicate risk, trend, or opportunity but never reveal underlying PHI. No central authority gains cross-institutional visibility. No one can surveil individuals. Yet population-wide intelligence begins to emerge.

As described in Section 3 ("Constitutional Protections for Patient-Controlled Privacy Domains"), Personal Privacy Networks and their Quantum Privacy Cells operate as patient-controlled domains rather than HIPAA-covered entities or institutional custodians, which means that any identifiable PHI they contain remains both cryptographically and constitutionally shielded from compelled disclosure. Sensitive behavioral, reproductive, and mental-health information used within QPC-bounded analytics is therefore legally irrecoverable unless the patient affirmatively authorizes disclosure. As a result, the population-level signals generated for preventive care, early-warning detection, and public-health response can guide action and policy without enabling surveillance, exposing individual identities, or permitting coercive access to personal medical information.

## From Rear-View Reporting to Continuous Preventive Guidance

Built on this foundation, the QPN transforms population health from a retrospective reporting exercise into a continuous, preventive, AI-driven, **interactive** network. When Quantum Privacy Cells (QPCs) detect early signs of concern—such as rising metabolic risk, deteriorating sleep stability, escalating stress trajectories, emerging cardiovascular strain, post-discharge fragility, or early markers of behavioral-health decline—those insights are surfaced immediately through Personal Privacy Networks (PPNs).

The PPN can then interact anonymously and in real time with the patient and their trusted network of clinicians, caregivers, family members, and connected devices—gathering additional encrypted information, validating signals, and delivering personalized decision support without exposing PHI to any external party. Clinicians receive early-warning insights directly within their existing workflows. Patients receive contextual, tailored guidance on their devices. Caregivers are notified in ways that respect permissions and legal rights. Community and social-service organizations can be prompted to intervene before a challenge escalates into a crisis.

Because all of this decision support is generated inside QPCs, each party sees only the limited information they are entitled to see. A clinician might receive a recommendation to adjust therapy or schedule outreach. An employer might see only de-identified risk-trend summaries at the population level. A public-health agency might see an emerging cluster of events in a region without knowing which specific individuals are affected.

## Coordinated, Multi-Stakeholder Preventive Workflows

QPN also provides the coordination fabric needed to act on these insights. When early-risk signals arise, they can automatically trigger multi-stakeholder workflows that span:

- clinicians and care teams,
- pharmacists and medication-management services,
- digital-therapeutic platforms,
- care-management and case-management programs,
- social-service and community organizations,
- employer benefit programs,
- public-health agencies, and
- family caregivers and trusted supporters.

Each operates entirely within its own Privacy Domain, using its own systems and permissions, but the overall effect is a unified preventive-care ecosystem rather than a patchwork of disconnected programs.

## Financial Flywheel for Preventive Care

Economically, these capabilities are deeply intertwined with the value-sharing mechanisms described elsewhere in this invention. Improvements in adherence feed directly into personalized plan design. Early detection reduces catastrophic claims inside global risk pools. Preventive engagement reduces long-term cost in ways that can be captured by personalized portable reinsurance instruments. Medication optimization strengthens therapy warranties and outcome-based agreements. Patient actions that reduce risk become fuel for personalized incentive ecosystems.

Taken together, the system creates a positive feedback loop:

- **early detection reduces costs,**
- **savings fund stronger incentives,**
- **incentives drive healthier behavior,**
- **healthier behavior lowers future risk,**
- **and improved risk profiles further reduce costs and improve prevention**.

Preventive care stops being an unfunded mandate and becomes a self-reinforcing economic engine.

## Public-Health Visibility Without Surveillance

For public-health authorities, QPN offers early-warning visibility without creating a surveillance state. Zero-knowledge analytics running across millions of QPCs can detect emerging infection clusters, environmental-exposure patterns, deteriorating chronic-disease trajectories, opioid-safety concerns, medication-safety failures, rising rates of mental-health crises, and other syndromic patterns—all without revealing any identifiable information.

Public-health agencies receive anonymized patterns, risk gradients, and regional trend signals. Unmasking a specific individual occurs only when lawful grounds exist—such as imminent risk of death, the need to dispatch emergency services, or the need to notify people exposed in a contamination event. Throughout, QPN preserves the privacy-protective ethos of HIPAA and related laws while delivering a level of timeliness and precision that traditional systems have never achieved.

## Anonymous, Real-Time Interaction with Patients and their Networks

Perhaps most importantly, QPN enables anonymous, real-time interaction with patients and their trusted networks. A PPN can receive a population-level safety alert and respond by asking the patient a few clarifying questions, pinging connected devices, inviting a caregiver to check in, or nudging the patient's clinician to review a new pattern—all without revealing the person's identity to regulators or any external system.

This closed-loop interaction supports both additional data gathering and validation, and also personalized decision support, alerts, and care-management interventions. It refines signals, reduces false positives, and directs help to where it is needed most, while preserving privacy and autonomy.

## Systemic Impact on Health and the Economy

As deployment scales, population health stops behaving like an after-the-fact analytics function and begins to operate as a living, continuous intelligence layer. Hospitalizations fall as deterioration is caught earlier. Chronic diseases stabilize sooner. Mental-health crises are intercepted before they become emergencies. Employer absenteeism and disability risk decline. Public expenditures shift from late-stage rescue to early-stage prevention. Population resilience improves, life expectancy rises, and workforce productivity increases.

In this model, preventive care is not a separate program. It is an emergent property of how the Quantum Privacy Network operates when millions of QPCs and PPNs continuously coordinate to keep people safer, healthier, and more stable in their daily lives.

## 16.0 A Nationwide Patient Safety, Public-Health & Research Network

### From Fragmented Safety Systems to a Unified Grid

While QPN provides the foundation for real-time preventive care, it also enables something even broader: a unified national safety, public-health, and research network that can replace dozens of fragmented programs with a single, coherent, privacy-preserving self-funding infrastructure.

For many years, the FDA, CDC, and state public health agencies have been responsible for monitoring the safety and effectiveness of drugs, biologics, devices, diagnostics, digital therapeutics, and other regulated products, as well as tracking emerging public health threats. To meet these responsibilities, the FDA operates a patchwork of specialized networks: Sentinel for drug safety, BEST for biologics, NEST for devices, SHIELD for lab-data harmonization, and MDEpiNet for post-market device epidemiology. Each program has its own governance, partners, data pipelines, and analytic frameworks. All are costly, data-hungry, and heavily dependent on delayed institutional feeds and voluntary reporting.

State and local public-health systems run their own overlapping reporting infrastructures that are often brittle, redundant, expensive to maintain, and burdensome for clinicians and hospitals—yet still fail to deliver timely, high-fidelity insight. The result is a safety and surveillance architecture that is fragmented, siloed, slow, error-prone, biased by what gets reported, and constrained by both privacy regulations and proprietary data ownership. The COVID pandemic proved just how broken the US public health data systems are.

### Quantum Privacy as the Common Safety Fabric

QPN replaces this fragmentation with a single global safety layer that continuously monitors patient outcomes, therapeutic performance, device behavior, and environmental exposures in real time, while keeping PHI locked inside QPCs under patient or institutional control. As a result, every care episode, medication event, diagnostic procedure, and device interaction contributes to a live, privacy-preserving evidence graph that can be reused concurrently for safety, quality, payment, public-health, and research without duplicative data collection or re-extraction.

The same multi-layered Quantum Privacy capabilities described in Section 3 apply here in a focused way. Data from hospitals, payers, pharmacies, labs, devices, digital therapeutics, and patient-generated sources can be analyzed where it already resides, inside QPCs and Privacy Domains, under Trust Blocks that encode all regulatory, contractual, and safety constraints. Privacy Pipes allow these domains to participate in national safety and public-health workflows without centralizing sensitive data. EasyAccess ensures that any clear-text access is minimal, granular, and fully auditable, while enabling the same workflows to simultaneously support benefit optimization, value-

based contracting, fraud detection, and utilization management without separate integrations.

In effect, QPN becomes a cryptographically governed substrate on which safety, surveillance, and research can operate continuously—without weakening privacy and without requiring legacy systems to be torn out or replaced. Because this same substrate is also used for routine care coordination, benefits administration, financial settlement, behavioral optimization, and cross-sector engagement, every additional safety or research use case operates at effectively zero marginal cost: it simply reuses the existing QPC-bounded infrastructure, data, and computation already in place for clinical, financial, and consumer workflows.

## Self-Funding National Patient Safety, Public-Health & Research Utility

The Nationwide Patient Safety, Public-Health & Research Network implemented on QPN is not a new, standalone system that must be funded and integrated from scratch. It is a person-centered utility layer that rides on top of dual-use infrastructure that already exists across the economy—EHR platforms, pharmacy systems, payer adjudication engines, cloud services, consumer apps, e-commerce platforms, financial rails, and digital-media ecosystems.

Within this architecture, Personal Privacy Networks (PPNs) and Enterprise Privacy Networks (EPNs) attach to existing APIs, message flows, and session interfaces, and then wrap those interactions in QPC-bounded, policy-enforced computation. No new central database is required; instead, QPN reuses the infrastructure that hospitals, payers, employers, platforms, and regulators already operate at internet scale, and simply adds a privacy-preserving, compliance-verified safety layer on top. In parallel, Quantum Privacy Accelerator and Exchange frameworks provide a mechanism for pooling savings and verified value across participants, while still relying on the same dual-use technical, legal, and organizational infrastructure.

Because QPN unifies care delivery, payments, public health, patient safety, and clinical research on a single privacy-preserving exchange, every workflow generates assets that are immediately reusable across all five domains at zero marginal cost. A prior-authorization interaction produces not only an authorization outcome, but also high-quality evidence about real-world effectiveness, adherence stability, benefit design performance, and safety trajectories. A medication-therapy-management intervention yields not only improved clinical outcomes, but also reusable analytics inputs for actuarial modeling, quality measurement, public-health surveillance, and trial eligibility—without any additional data feeds or integrations. The same is true for referrals, social-needs interventions, device telemetry, and lifestyle-signal optimization: once captured and

computed inside QPCs, the resulting signals can be reprocessed, recombined, and reused across all authorized use cases without new data acquisition or infrastructure spend.

This zero-marginal-cost reuse is amplified by QPN's cross-sector design. Health-relevant context—nutrition choices, financial stress indicators, mobility and transportation patterns, workplace dynamics, and digital-media engagement—flows through people's existing digital lives. QPN does not require e-commerce, financial institutions, transportation networks, or entertainment platforms to become health systems. Instead, PPNs and EPNs leverage the rights and permissions individuals and institutions already hold to execute privacy-preserving, zero-knowledge interactions with these ecosystems, extracting only the minimal, risk-relevant eligibility or personalization signals needed to improve health, safety, and well-being. The underlying sectors never see PHI or clinical risk scores; QPCs perform all health-related computation inside the user's Privacy Domain and release only de-identified or zero-knowledge outputs back into the network.

In this model, the Nationwide Patient Safety, Public-Health & Research Network becomes self-funding. Today's system burns trillions of dollars annually on avoidable hospitalizations, redundant tests, administrative friction, payment errors, fraud, suboptimal benefit design, delayed care, and preventable adverse events. QPN converts that waste into a continuous stream of measurable, monetizable efficiencies: fewer preventable errors, optimized therapies, earlier interventions, reduced readmissions, better medication adherence, fewer denied claims, and more precise targeting of high-value services. The verified savings and incremental revenue that result—and that can be tracked and attributed with cryptographic provenance through the Privacy Network Exchange—vastly exceed the incremental operating costs of the network itself.

Because QPN's marginal operating cost per additional patient, clinician, workflow, or safety use case approaches zero, the rational economic design is to make core Nationwide Patient Safety, Public-Health & Research services freely available at the point of use. Payers, employers, health systems, and public agencies can fund the shared infrastructure out of captured savings and verified value, while patients, caregivers, clinicians, and communities experience it as a universal, no-cost utility: always on, always privacy-preserving, and always working in the background to prevent harm, improve outcomes, and accelerate research.

In certain embodiments, these savings and value streams are pooled through Quantum Privacy Accelerator structures and tokenized Exchange mechanisms, enabling automated redistribution of verified value back to the participants who created it—patients, clinicians, caregivers, innovators, and public-benefit programs—without compromising privacy or regulatory compliance.

In all embodiments, the core principle is the same: by unifying safety, public health, research, and everyday care on a single Quantum Privacy Network that reuses existing dual-use infrastructure and operates at zero marginal cost, the Nationwide Patient Safety, Public-Health & Research Network becomes both economically self-sustaining and universally accessible.

## Regulatory Authorities and Legal Pathways

Existing law already provides the regulatory pathway for such a network.

The FDA has broad authority to impose safety measures as a condition of allowing regulated products to be marketed across state lines. It routinely requires participation in REMS programs, post-market surveillance, real-world evidence collection, and ongoing safety monitoring for drugs, biologics, devices, diagnostics, and digital therapeutics.

At the same time, HIPAA's Public Health Exception (45 CFR § 164.512) authorizes all HIPAA-covered entities—hospitals, payers, PBMs, pharmacies, labs, and clinicians—to disclose PHI without patient authorization for public-health and safety purposes, including adverse-event detection, tracking of FDA-regulated products, product recalls, outbreak monitoring, and a wide range of surveillance activities. These disclosures may be made not only to government agencies, but also to entities acting on their behalf for authorized public-health functions.

Taken together, these authorities enable HIPAA-covered entities to send safety-relevant data to a self-funding, decentralized, patient-centered QPN-based safety network, so long as the network is performing FDA-, CDC-, or state-authorized public-health functions. Once data enters the network, it can also be routed—under the Patient Right of Access (45 CFR § 164.524)—into each individual's Personal Privacy Network. At that point, the patient gains direct control. The information is no longer subject to HIPAA, and can safely participate in privacy-preserving analytics, personalized decision support, and research workflows under patient-controlled authorization. QPN's cryptographic protections ensure that privacy and data security are substantially stronger than in many of the legacy systems from which the data originated.

## Unifying and Enhancing Existing FDA Safety Programs

Within this framework, QPN can combine, enhance, or eventually replace the FDA's existing safety networks. Sentinel's retrospective drug-safety analyses, BEST's biologics surveillance, NEST's device-safety monitoring, SHIELD's lab-data harmonization, and MDEpiNet's device registries can all be re-expressed as real-time, zero-knowledge analytics operating across QPCs.

Instead of pulling delayed, institution-level data into centralized repositories, QPN supports continuous safety computation where the data already resides and emits only

anonymized signals or privacy-bounded summaries. The result is a unified, global, real-time safety and observational-research layer that is both more effective and dramatically less expensive to operate.

## A Free, Personalized Patient-Safety Service

To patients and clinicians, this same infrastructure appears as a free, highly personalized safety service. It continuously monitors for dangerous drug interactions, metabolic instability, behavioral-health deterioration, environmental hazards, post-discharge complications, adherence breakdowns, device anomalies, and early symptoms of emerging disease.

When something concerning appears, the network can interact anonymously with the patient and their trusted circle. A PPN can:

- ask brief symptom-check questions,
- collect additional encrypted signals from devices,
- invite a caregiver or family member to check in,
- provide personalized safety alerts and decision support, and
- nudge clinicians or care teams to review the situation.

All of this occurs without revealing the patient's identity to regulators or any external party, unless there is a clear, lawful need—such as dispatching emergency services or notifying someone of acute risk.

Because the service is free, privacy-preserving, and substantially improves patient safety, adoption by clinicians and patients is likely to be enthusiastic. Even if adoption were slow, the FDA could still require participation as a condition for prescribing certain drugs, participating in REMS, marketing specific devices or biologics, deploying digital therapeutics, or using AI-driven clinical decision support tools.

## A Global Public-Health and Research Grid Without Surveillance

From the perspective of public-health agencies, the same network functions as a powerful, non-surveillant early-warning grid. Zero-knowledge analytics inside QPCs detect:

- emerging infection clusters,
- environmental risk patterns,
- chronic-disease deterioration,
- opioid-safety and substance-use signals,
- medication-safety failures and rare adverse events,
- mental-health crises and suicide-risk patterns,
- food-supply contamination signals,
- syndromic-surveillance indicators, and
- possible biothreat emergence.

Agencies see population-level signals, geographic and demographic patterns, and changes in risk over time—but not the identities of individuals. Unmasking is reserved for situations where legal standards are met – and only for purposes that benefit the patient, and don't violate their privacy – such as imminent danger or necessary notification of exposed individuals.

As described in the subsection "Constitutional Protections for Patient-Controlled Privacy Domains," the patient's Personal Privacy Network (PPN) and its Quantum Privacy Cell (QPC) are both legally and technically incapable of disclosing clear-text PHI without the patient's affirmative authorization. Compelling a patient to authorize decryption would violate the Fifth Amendment, and the QPC itself cannot comply on its own. As a result, even when population-level patterns inform public-health response, individual identities remain cryptographically and constitutionally irrecoverable unless the patient chooses to permit unmasking. This safeguard ensures that national-scale safety networks enhance public health without enabling surveillance, coercive disclosure, or state overreach into private medical information.

## A Nationwide Privacy-Preserving Research Platform

The same infrastructure that powers national-scale patient safety and public-health intelligence also serves as a continuously operating, privacy-preserving observational-research platform for the NIH, academic medical centers, pharmaceutical developers, private-sector clinical-research networks, CROs, and global consortia. Because all computation occurs inside Quantum Privacy Cells (QPCs), real-world data—from clinical encounters, home environments, connected devices, digital therapeutics, and everyday behavior—can be analyzed as encrypted signals rather than pooled into centralized databases. This enables:

- **real-time Phase 4 and post-market studies** with far higher fidelity and dramatically lower operational burden,
- **pragmatic and confirmatory trials** that run seamlessly across diverse clinical settings,
- **adaptive registries** that update continuously rather than annually or episodically, and
- **continuous post-market evaluation** across heterogeneous populations without exposing PHI.

This architecture delivers distinct advantages to every participant in the research ecosystem. **NIH and academic medical centers** gain access to national-scale, high-quality real-world evidence without navigating restrictive data-use agreements or risking privacy violations. **Pharmaceutical and biotech sponsors** can validate therapeutic performance and safety in real time, accelerating confirmatory trials and reducing post-

market uncertainty. **CROs and private research networks** can execute studies at lower cost and with far greater recruitment reach because eligibility, consent, adherence monitoring, adverse-event reporting, and follow-up can all be handled directly within each patient's Personal Privacy Network (PPN). **Clinicians and health systems** can offer research participation as an effortless extension of routine care—making true Clinical Research As A Care Option (CRAACO) possible at national scale.

Patients benefit most. They can opt into research with a few taps, receive personalized decision support, maintain control over their data, and contribute to medical knowledge without sacrificing privacy or autonomy. Researchers, in turn, gain unprecedented volumes of high-fidelity, privacy-preserving evidence generated passively and continuously as a by-product of everyday healthcare and daily life.

Together with the cryptographic trust architecture described in **Section 3**, the preventive-intelligence framework detailed in **Section 15**, and the nationwide safety and public-health network outlined in **Section 16**, this research platform becomes part of a single, synergistic ecosystem. Every clinical encounter, safety signal, preventive-action event, benefit interaction, or digital engagement automatically produces high-fidelity, privacy-preserved evidence that can be reused—continuously and at zero marginal cost—for research. This eliminates the redundant data extraction, manual chart review, recruitment churn, site-activation delays, and fragmented follow-up that make traditional studies slow and prohibitively expensive. As a result, large-scale clinical research—including Phase 4 trials, pragmatic trials, registries, and real-world evidence programs—can be conducted at **one-tenth the cost** of today's paradigms, while delivering higher data quality, stronger regulatory compliance, and far greater participation. In this unified model, clinical research ceases to be a separate, burdensome system and becomes a natural extension of care, safety, and public-health workflows—accelerating therapeutic innovation while protecting the privacy, autonomy, and rights of patients.

## Fast Path to Nationwide Deployment

All of this can be deployed quickly using existing law and existing systems. HIPAA § 164.512 authorizes disclosure for public-health and safety purposes; HIPAA § 164.506 permits disclosures for treatment and payment; HIPAA § 164.524 ensures patients can receive copies of their data and route it into their PPNs; and the FDA's existing authorities allow it to condition interstate distribution of regulated products on participation in appropriate safety systems.

Hospitals, payers, PBMs, pharmacies, and labs already possess both the legal right—and in many contexts, the obligation—to participate in such a network. QPN simply provides the missing technical and governance infrastructure to make participation safe, efficient, and value-creating for everyone.

**Transformative Impact on Safety, Public Health, and Research**

The result is a single, coherent infrastructure that meets multiple missions at once:

- **a free, globally scalable patient-safety service,**
- **a unified national public-health grid,**
- **a real-time FDA-regulated safety-surveillance platform,**
- **a continuous observational-research network, and**
- **a privacy-preserving data ecosystem governed, at its core, by patients themselves.**

Instead of dozens of siloed, underperforming systems struggling to keep up with modern health risks, the country gains one cryptographically governed, self-improving network that continuously enhances safety, accelerates therapeutic innovation, strengthens public health, and produces an unparalleled stream of real-world evidence.

If deployed at scale, a QPN-enabled safety and research network would inevitably become the most powerful patient-safety, public-health, and clinical research system in the world—achieving a level of responsiveness, precision, and privacy protection that no government agency or private company could build on its own.

## 17.0 Personalized Behavioral Health & Mental-Health Ecosystems

Behavioral health is one of the most sensitive, fragmented, and structurally underserved domains in the U.S. healthcare system. Despite major investment in digital therapeutics, teletherapy, collaborative-care models, crisis-response programs, and population-level behavioral-health initiatives, outcomes remain inconsistent because no existing infrastructure can safely unify the clinical, social, environmental, family-context, and engagement data required for true personalization. Privacy laws such as HIPAA, 42 CFR Part 2, and state mental-health protections appropriately restrict disclosure of sensitive information—but they also make cross-organizational coordination nearly impossible, preventing the early detection, continuous support, and crisis-avoidance workflows that behavioral health most urgently requires. As a result, behavioral health remains siloed, reactive, and difficult to integrate into broader care pathways.

The Quantum Privacy Network (QPN) removes these barriers. By anchoring all behavioral-health computation inside patient-controlled Quantum Privacy Cells (QPCs), QPN makes it possible—for the first time—to unify clinical care, digital mental-health tools, community and social-support networks, crisis-management workflows, and preventive engagement into a single, privacy-preserving ecosystem. Because QPCs are both technically and legally incapable of disclosing clear-text behavioral-health information without the patient's explicit authorization (see Section 3, "Constitutional Protections for Patient-

Controlled Privacy Domains"), individuals can participate fully and honestly without fear of surveillance, stigma, discrimination, or coerced disclosure.

This architecture enables a new paradigm in which early-warning signals, daily-life context, environmental stressors, digital-engagement patterns, caregiver insights, and clinical markers can interact safely and continuously—allowing behavioral-health support to become timely, personalized, anticipatory, and deeply human-centered, while remaining fully compliant with all federal and state privacy laws.

## A Privacy Foundation for Mental-Health Engagement

As further detailed in Section 3, the legal and cryptographic irreversibility of patient-controlled Privacy Domains is especially critical in behavioral and mental health. A patient's QPC cannot decrypt or disclose sensitive behavioral-health or reproductive-health information without an affirmative authorization from the patient—and compelling such authorization would violate longstanding Fifth Amendment doctrine. This guarantees that individuals can safely share their most vulnerable reflections, symptoms, triggers, and disclosures without fear of institutional misuse, legal exposure, employment consequences, or state-level scrutiny. The result is a level of psychological safety no traditional health-IT system can provide, enabling earlier self-disclosure, more accurate symptom reporting, and much deeper engagement with preventive and therapeutic mental-health workflows.

### Why Behavioral-Health Integration Has Historically Been Impossible

Behavioral health has always been siloed because:

1. **42 CFR Part 2 prohibits redisclosure of substance-use data**: Existing systems cannot enforce redisclosure constraints across multiple organizations or across AI systems.
2. **Behavioral-health information cannot legally be co-mingled**: with primary-care, employer, school, or payer data in traditional data lakes or EHR integrations.
3. **Mental-health and SDOH data often originate outside medical systems**: (peer support groups, community programs, crisis lines, schools, workplaces).
4. **Stigma and safety risks demand more protections** than existing privacy frameworks can enforce.
5. **AI models trained centrally on behavioral-health data create serious harms**: including reidentification, bias, inference attacks, and discrimination.
6. **Providers, payers, digital therapeutics & community organizations lack shared rails** for coordinated behavioral-health workflows.

As a result, behavioral health remains disconnected, inconsistent, and difficult to personalize. QPN removes these structural barriers through cryptographically enforced privacy domains

## Privacy-Preserving, Multi-Domain Behavioral-Health Integration

QPN allows every behavioral-health interaction—clinical, digital, community, environmental, or social—to occur **inside a cryptographically bounded Privacy Domain**, where:

- data is never exposed or centralized
- rights and redisclosure restrictions are enforced automatically
- AI operates in privacy-preserving execution cleanrooms
- only role-appropriate information is shared
- a reversible audit trail ensures accountability without stigma
- multi-stakeholder coordination occurs without revealing sensitive details

This allows mental-health data to coexist with medical, social, and environmental context while **remaining isolated, protected, and strictly governed**.

## Personalized Behavioral-Health Pathways

QPN enables the construction of individualized behavioral-health pathways that adjust dynamically to a person's clinical state, preferences, risk factors, and life events. Examples include:

- automated identification of unmet behavioral-health needs
- proactive nudges, reminders, and follow-up coordination
- personalized engagement strategies based on evidence and context
- integrated referrals between primary care, psychiatry, psychology, and digital therapeutics
- privacy-preserving medication monitoring
- task routing across clinicians, care teams, case managers, and AI agents

Each workflow is orchestrated through EasyAccess Threads, allowing seamless, cross-organizational coordination with no backend integrations.

## Integration with Digital Therapeutics & AI-Driven Mental-Health Agents

QPN provides the environment needed for safe deployment of digital mental-health tools, including:

- Cognitive Behavioral Therapy (CBT)-based digital therapeutics
- AI-driven behavioral coaches
- emotion-aware conversational models
- exposure-therapy tools

- sleep, anxiety, or depression management programs
- mindfulness and resilience training apps
- addiction-recovery applications

Because these tools operate inside Quantum Privacy Cells, they can:

- access behavioral context without exposing data
- adapt strategies based on personal evidence graphs
- escalate to clinicians only when appropriate
- respect redisclosure constraints
- maintain full explainability and lineage
- ensure safe, bias-checked AI reasoning

This enables **safe, compliant, deeply personalized mental-health AI** at scale.

## Crisis Prediction, Safety Monitoring, and Escalation Pathways

The Quantum Privacy Network supports early identification of behavioral-health deterioration and provides structured, privacy-preserving escalation.

Signals may include:

- medication non-adherence
- worsening PHQ-9 or GAD-7 scores
- changes in speech patterns or engagement behaviors
- isolation markers
- sleep disruption
- social or financial stress signals
- community-reported concerns
- environmental risk factors

When risks cross thresholds, QPN can orchestrate:

- secure alerts to authorized clinicians
- involvement of caregivers or trusted individuals
- escalation to crisis lines or mobile crisis teams
- engagement of community resources
- integration with safety-planning workflows

All without revealing unnecessary details or violating 42 CFR Part 2 protections.

## Family, Caregiver, and Peer-Support Integration

Behavioral-health recovery is relational. Yet caregivers and peer networks are routinely excluded for privacy reasons.

QPN enables role-filtered participation:

- caregivers can help coordinate appointments
- peers can support adherence or crisis de-escalation
- family members can be informed of safety concerns (with patient consent)
- clinicians can collaborate across organizations
- case managers can assist with housing, food, or employment barriers

All access is governed by cryptographic consent lineage and restricted to the specific information each participant is authorized to see.

## Behavioral-Health Quality, Attribution, and Value-Based Incentives

QPN's Proof-of-Trust (PoT) and Trust Block lineage make it possible to measure behavioral-health outcomes and attribute value across stakeholders:

- digital therapeutics
- community programs
- peer-support networks
- therapists and psychiatrists
- primary-care clinicians
- case managers
- employers and schools

This enables **value-based mental-health models** where compensation aligns with improved outcomes, not service volume.

It also unlocks standardized, privacy-preserving metrics for:

- symptom reduction
- functional improvement
- crisis avoidance
- hospitalization prevention
- adherence support
- quality of life

This transforms behavioral health from a fragmented cost-center into a measurable, improvable system.

## Mental-Health Equity and Bias-Resistant AI

QPN provides the mechanisms necessary for equitable mental-health AI models:

- zero-knowledge fairness testing
- bias-resistant model selection
- jurisdiction-based constraint enforcement
- explainability through Trust Block lineage
- community-specific calibration

- prevention of discriminatory inference

These protections cannot be implemented in centralized AI architectures but are native to QPC-bounded computation.

### Behavioral-Health Integration as a Core Pillar of Personalized Healthcare

Sections 1.0–16.0 established the foundation for personalized care coordination, value-based benefit design, affordability, risk pooling, reinsurance, medication management, and social support.

Section 17.0 extends this foundation into behavioral health, establishing the first **national mental-health ecosystem** where clinical, digital, social, and environmental factors are integrated safely and dynamically.

The result is a system in which:

- mental health is treated with the same precision & personalization as physical health
- individuals receive continuous, preventive, context-aware support
- stigma is reduced through privacy-preserving computation
- community resources are first-class components of care
- crises are predicted and prevented, not reacted to
- AI enhances—not replaces—human connection and judgment

Through QPN, behavioral health becomes both **coordinated and fundamentally human**, finally integrated as a core dimension of whole-person care.

## 18.0 Federated Genomics & Precision-Medicine Networks

Genomics lies at the center of the next era of medicine. It is the foundation for personalized risk prediction, early detection, therapeutic selection, rare-disease diagnosis, pharmacogenomics, cell and gene therapy eligibility, and lifelong preventive care. Yet despite decades of scientific progress, genomics has not been integrated into mainstream healthcare at scale. The reason is structural: no existing architecture can safely, legally, or operationally unify genomic data with the broader clinical, behavioral, environmental, and social context required for precision medicine.

The Quantum Privacy Network (QPN) provides—for the first time—a national infrastructure that enables **privacy-preserving, federated, AI-optimized genomics and precision-medicine networks**. It allows genomic insights to be used continuously, safely, and dynamically across a person's lifetime, without exposing raw genomic sequences, without creating centralized risk, and without violating the complex mosaic of genetic privacy laws.

Through QPN, genomics becomes a first-class component of personalized healthcare, integrated seamlessly into care delivery, benefits, prevention, behavioral health, research, and long-term care pathways.

## Why Genomics Cannot Be Integrated Using Existing Systems

Traditional healthcare infrastructures cannot support safe, legal, or effective genomic integration because:

1. **Genomic data is uniquely identifying:** Even small genomic fragments can re-identify individuals with high fidelity.
2. **Genomics is legally constrained:** HIPAA, GINA, GIPA, state privacy laws, employment protections, insurance rules, and research protocols impose incompatible constraints on handling genomic information.
3. **No existing interoperability standard supports genomic privacy:** FHIR Genomics and research-data platforms require centralized pooling—non-compliant with modern privacy laws.
4. **Genomics requires cross-domain combination with PHI, claims, social, environmental, and behavioral context** to be clinically useful—yet every combination increases privacy risk.
5. **AI models trained on central genomic repositories pose catastrophic risks**, including discrimination, inference attacks, and irrevocable privacy exposure.
6. **Precision-medicine workflows span dozens of organizations** (labs, specialists, manufacturers, research networks, payers), none of which share secure rails.

Thus, genomics remains siloed, underused, and often isolated from routine medical care.

The Quantum Privacy Network breaks through each of these barriers.

## Federated Genomics Inside Quantum Privacy Cells

QPN enables genomic analysis and precision-medicine computation to occur **inside Quantum Privacy Cells (QPCs)**, where raw genomic sequences:

- are never exposed
- are never centralized
- are never shared with payers, employers, or researchers
- cannot be copied, exported, or used for unauthorized inference

Instead of moving genomic data, QPN distributes computation *to* the data. All genomic reasoning occurs within privacy-bounded environments that enforce:

- attribute-level consent
- redisclosure rules

- jurisdiction-specific genetic-privacy mandates
- strict access to derived insights only
- reversible audit trails via Trust Blocks
- zero-knowledge proof validation

This is the first architecture capable of protecting genomics at the level required for widespread clinical use.

## AI-Optimized Precision-Medicine Pathways

Within QPN, federated genomics becomes a continuous, personalized input into care pathways. AI agents can analyze:

- rare-disease markers
- pharmacogenomics
- disease-risk profiles
- companion-diagnostic criteria
- tumor sequencing data
- hereditary-risk patterns
- eligibility for gene or cell therapies
- longitudinal genetic risk trajectories

—all within privacy-preserving computation environments.

The result is a dynamic precision-medicine ecosystem where:

- preventive care is tailored
- treatment selection is personalized
- medication safety is optimized
- follow-up intervals are individualized
- lifestyle and behavioral interventions are genetically informed

without exposing genomic data to insurers, employers, or unauthorized entities.

## Population-Level Genomic Insights Without Centralization

Public health, research networks, and population-health organizations can access **zero-knowledge, federated genomic analytics** that reveal patterns such as:

- disease-risk clusters
- pharmacogenomic distributions
- rare-disease prevalence
- population-level gene–environment interactions
- health-equity insights
- precision-prevention opportunities

—all without receiving or viewing any individual's genomic sequence or identifiable PHI.

This enables large-scale genomic research, surveillance, and equity-monitoring **without creating genomic databases** vulnerable to hacking, reidentification, or misuse.

QPN standardizes genomic consent and ethical governance through:

- attribute-level consent controls
- role-specific genomic insight sharing
- multi-stakeholder Human-managed Trust Authorities (HTAs)
- reversible audit trails
- zero-knowledge validation of allowed uses
- multi-jurisdiction inheritance of genetic privacy rules
- automated enforcement of "need-to-know" policies

Genomic insights become legally and ethically safe to use in routine care—for the first time.

## Precision Therapeutics, Gene Therapy & Personalized Treatment Warranties

QPN enables safe, compliant coordination of:

- cell and gene therapy eligibility
- biomarker-driven companion diagnostics
- precision oncology workflows
- gene-editing follow-up monitoring
- manufacturer-payer outcomes-based warranties
- real-world evidence tracking

When therapy success is tied to specific genetic markers, QPN ensures:

- eligibility is validated without exposing genomic sequences
- outcomes monitoring is private and auditable
- manufacturers can offer warranties without receiving PHI
- payers can verify performance without violating privacy laws

This replaces complex, manual, risky genomic workflows with automated, privacy-preserving arrangements.

QPN **allows researchers to run analytics on patient genomes inside privacy domains** where:

- raw sequences remain cryptographically sealed
- identifiers are never revealed
- query outputs are zero-knowledge bounded
- training data cannot be exfiltrated
- fairness and bias tests are cryptographically enforced

**Researchers receive insights, not data**. Individuals retain full control of their genomes via their PPN. This unlocks a new era of safe, scalable genomic research.

## Integration With Environmental, SDOH, Behavioral, and Lifestyle Context

Precision medicine requires the linking and analysis of comprehensive patient data, both on a population scale and for each individual patient to support personalized decision support, diagnostics, and care management:

- genomics
- environment
- behavior
- social determinants
- nutrition
- lifestyle patterns
- family history
- mental-health context

Since genomic data is inherently identifying, it can't be de-identified even in theory – and attempting to do so would so defeat the purpose of enabling precision-personalized care. Thus, the traditional tokenization and cleanroom approaches to privacy are fundamentally inadequate.

QPN is the only infrastructure capable of integrating these safely and continuously. This allows:

- individualized early detection
- personalized prevention
- targeted lifestyle interventions
- environmental-risk mitigation
- cross-domain risk modeling
- real-time adaptation as patient context changes

Precision medicine becomes **living, dynamic, adaptive**, not static. Through the Quantum Privacy Network, genomics becomes:

- safe
- federated
- AI-optimized
- integrated with care and prevention
- ethically governed
- legally compliant
- economically scalable
- personalized to every individual

It becomes a driver of better outcomes, earlier detection, optimized therapy, and lifelong health.

## 19.0 Self-funding Real-World Evidence & Continuous Learning Networks

Modern healthcare depends on real-world evidence (RWE). It informs clinical guidelines, regulatory decisions, benefit design, population-health strategies, value-based contracts, post-market surveillance, patient-safety systems, and emerging AI-driven innovation. Yet traditional RWE systems are slow, limited, retrospective, and fragmented because they depend on centralized data pooling, delayed claims feeds, partial clinical records, and proprietary data brokers that cannot generate or integrate real-time, patient-centered information from across the healthcare ecosystem.

The Quantum Privacy Network (QPN) enables—for the first time—a **self-funding, continuously learning, privacy-preserving national RWE infrastructure** that synthesizes clinical, behavioral, genomic, environmental, social, and contextual signals directly from patient, clinician, caregiver, and device interactions. These signals are captured inside Personal and Enterprise Privacy Networks with **full provenance, cryptographically enforced rights, and zero-knowledge privacy guarantees**, creating a unified, high-fidelity evidence graph unavailable anywhere else in the healthcare system.

Because QPN leverages **dual-use infrastructure**—existing EHR portals, payer systems, PBM accounts, laboratory portals, pharmacy systems, digital therapeutics, community organizations, and patient-held rights—no institution needs to modify its backend systems or create new integrations. The evidence network grows organically as patients and clinicians participate in normal workflows. Every new event, record, interaction, or device signal becomes part of a **privacy-preserving, zero-marginal-cost evidence engine** that can be reused indefinitely without compromising privacy, regulatory compliance, or commercial rights.

Unlike centralized data repositories or traditional federated networks, QPN generates **new classes of real-time data** that cannot be captured today: contextual behavioral signals, caregiver insights, device telemetry, decision pathways, affordability interactions, social-support engagement, value-based incentives, digital-therapeutic performance, real-time symptom changes, and environmental risk signals. Because these data streams are cryptographically bounded, richly contextual, fully provenance-linked, and continuously reusable, they become **exponentially more valuable** to providers, payers, manufacturers, public-health agencies, researchers, and AI systems—while remaining entirely under patient control.

The Privacy Network Exchange (PNX) allows this evidence to be **reprocessed, repurposed, and recombined at zero marginal cost**, enabling a self-funding economic model: every workflow that improves coordination, reduces waste, accelerates prior authorization, prevents adverse events, or improves medication adherence generates savings that directly finance additional analytics, population-health improvements, and continuous learning.

Through QPN, federated RWE becomes real-time, clinically actionable, economically sustainable, and safely accessible for every authorized stakeholder—patients, clinicians, caregivers, researchers, public-health agencies, and value-based care participants. It forms the backbone of a national continuous-learning health system where the quality of care improves with every patient interaction, and where privacy-preserving intelligence becomes a shared, renewable resource that benefits the entire ecosystem.

## Why Real-World Evidence Has Been Limited, Incomplete, and Risky

Traditional RWE ecosystems rely on centralized data pools, commercial data brokers, payer extracts, research repositories, and cloud-based analytics platforms. These models face several insurmountable limits:

1. **Centralized data registries violate privacy constraints:** They cannot safely combine PHI, genomic data, behavioral patterns, payer data, and social-context information.
2. **Data brokers operate with opaque, non-transparent data flows:** Patients cannot meaningfully consent; clinicians and health systems cannot fully trust the provenance.
3. **Real-world data (RWD) is fragmented across hundreds of systems:** EHRs, claims, labs, pharmacies, wearables, digital therapeutics, and community platforms produce incompatible data.
4. **Regulatory barriers restrict data sharing:** HIPAA, 42 CFR Part 2, GINA/GIPA, CPRA/CPA, EU AI Act, and payer-contractual rules prohibit broad pooling.
5. **AI models trained on pooled data are privacy-unsafe:** They are vulnerable to inversion attacks, reidentification, membership inference, and discriminatory bias.
6. **RWE is often retrospective and slow:** Lagged claims data and incomplete clinical information limit relevance for real-time decision-making.

QPN solves each of these challenges through federated, cryptographically bounded computation.

## QPN as a Global Self-funding Federated RWE Infrastructure

QPN transforms RWE from a slow, retrospective, silo-dependent activity into a **continuous, real-time, federated learning process**.

Inside the Quantum Privacy Network:

- data never leaves personal or enterprise privacy domains
- computation moves to the data
- analysis occurs inside QPC-bounded privacy cleanrooms
- only zero-knowledge outputs or privacy-bounded aggregates are shared
- lineage and provenance are immutably recorded via Trust Blocks
- consent and rights are cryptographically enforced
- multi-jurisdiction policies (HIPAA, 42 CFR Part 2, GINA, state laws) are inherited at run-time

This architecture enables RWE that is **complete, compliant, dynamic, and unbiased**.

The Quantum Privacy Network supports federated, continuously learning Real World Evidence (RWE) across the entire healthcare ecosystem:

- **Providers**: Care-pathway optimization, risk prediction, quality improvement.
- **Payers & Employers**: Benefit design, value-based contracting, affordability strategies.
- **Pharmaceutical & biotech manufacturers:** Post-market surveillance, real-world performance, outcomes-based warranties.
- **Digital therapeutics & AI tools:** Continuous validation, bias detection, safety monitoring, model updates.
- **Public health agencies**: Zero-knowledge population-level epidemiology and risk tracking.
- **Research networks**: Privacy-preserving, federated real-world studies without centralized data sharing.
- **Community & social networks:** Impact assessments for social determinants and community health programs.

Because QPN provides a unified evidence graph that spans clinical, behavioral, genomic, environmental, and social data—**without exposing any of it**—it becomes the first lawful infrastructure for continuous real-world learning.

## Zero-Knowledge Evidence Derivation & Privacy-Preserving Validation

A core breakthrough of QPN is that RWE does not require revealing raw data via the use of:

- zero-knowledge proofs

- constraint-aware federated computation
- encrypted model execution
- privacy-bounded inference
- Trust Block lineage
- attribute-level consent

The Quantum Privacy Network enables:

- continuous outcome measurement
- anonymous safety monitoring
- precision pharmacovigilance
- disease-progression modeling
- therapy-performance validation
- fairness & bias detection
- comparative-effectiveness analytics
- continuous model retraining

—all without revealing PHI, genomic sequences, claims data, or behavioral insights. This overcomes the barriers that have prevented real-time RWE adoption in regulated domains.

## Real-World Performance Monitoring for Therapies, Devices & Digital Tools

QPN enables continuous real-world performance evaluation of:

- pharmaceuticals
- gene and cell therapies
- medical devices
- digital therapeutics
- AI-powered clinical tools

Manufacturers, regulators, and payers can:

- validate outcomes
- detect safety signals
- measure adherence and engagement
- assess value-based performance
- adjust risk-sharing agreements
- trigger therapy warranties (see Section 16.0)
- optimize benefit design
- evaluate comparative effectiveness

All of this occurs entirely inside privacy-preserving computation domains.

## Federated AI Training & Continuous Improvement Without Data Sharing

AI models can be continuously trained, calibrated, tested, validated, and improved using federated learning techniques across the QPN, where:

- data never leaves the privacy domain
- updates are privacy-bounded
- model weights cannot leak PHI
- bias-detection is cryptographically enforced
- auditability is guaranteed via Trust Blocks
- explainability is available where required
- multi-jurisdiction constraints are enforced at inference time

This enables **safe national AI models** for diagnosis, risk prediction, triage, population health, mental health, chronic disease, care navigation, and digital therapeutics that meet modern standards for safety, fairness, and accountability.

## RWE-Driven Value-Based Care & Contracting

QPN enables value-based arrangements that are accurate, fair, and legally enforceable:

- outcome-based pricing
- complexity-adjusted reimbursement
- value-sharing with community organizations
- payer-manufacturer risk arrangements
- digital-therapeutic performance contracts
- therapy warranties
- employer-driven value contracting
- population-level incentive structures

Because every data point is:

- cryptographically validated
- lineage-tracked
- jurisdiction-compliant
- securely derived

value-based models become transparent, auditable, and impossible to manipulate.

## Federated RWE as a Pillar of a Global Personalized Health Marketplace

Sections 1–18 establish the unified architecture for personalized health, genomics, behavioral care, affordability, risk pooling, and community integration.

Section 19 extends this architecture into continuous, federated learning that powers:

- better clinical decisions
- safer AI

- more effective therapies
- smarter benefit design
- predictive population-health models
- faster research cycles
- more accurate value-based contracts
- national-level health improvement

QPN transforms RWE from a fragmented, retrospective, manual process into a **living, learning, real-time intelligence system** for the entire country.

It is the foundation for a continuously improving healthcare system—one where each encounter, each therapy, each decision, and each patient interaction strengthens the collective intelligence of the ecosystem, without sacrificing privacy, ethics, or trust.

## 20.0 AI Personal Health Agents

Coordinating healthcare today is overwhelming for patients, clinicians, caregivers, and care teams. Patients must navigate fragmented portals, inconsistent benefits, opaque prices, disconnected services, time-consuming paperwork, and manually coordinated communications across dozens of organizations. Clinical teams spend enormous time on non-clinical work, navigating prior authorizations, referrals, benefits, medication access, appeals, and follow-up tasks—often without the data or tools needed for timely, informed decisions.

The fundamental reason care navigation fails is structural: no existing system has the authority, data access, privacy protections, or cross-organizational workflow capability to perform navigation on behalf of patients or clinicians. Even modern AI assistants cannot safely interact with PHI, payer systems, PBMs, pharmacies, labs, or community networks across organizational boundaries.

The Quantum Privacy Network (QPN) enables, for the first time, **Personal Health Agents (PHAs)**—AI-driven, privacy-preserving assistants capable of orchestrating care, benefits, communication, adjudication, and coordination across the entire healthcare ecosystem. These agents operate under cryptographic trust constraints, inside privacy-bounded execution domains, and with full lineage, accountability, and policy enforcement.

Personal Health Agents transform care navigation from a manual, fragmented burden into a fully automated, AI-optimized capability that operates on behalf of the patient, clinician, family, and care team.

## Why Care Navigation Has Never Been Automatable

In traditional healthcare architecture, AI agents or automated workflows cannot coordinate care because:

1. **PHI cannot legally move across systems or vendors**: AI cannot safely operate across EHRs, payers, PBMs, labs, pharmacies, or community organizations.
2. **Identity and authorization are fragmented:** No unified identity system exists to represent a patient—and their rights—across all participants.
3. **Benefits and eligibility systems are opaque**: There is no consistent or trusted way to compute real-time out-of-pocket costs or coverage rules.
4. **Clinical and social care pathways span dozens of organizations**: And none share secure rails for workflow coordination.
5. **AI lacks reliable, privacy-preserving access to evidence graphs:** Genomics, SDOH, behavioral data, claims, and clinical histories remain siloed.
6. **No shared governance framework exists:** to manage safety, fairness, oversight, and explainability of cross-organizational AI.

As a result, AI assistants remain limited to shallow, non-clinical tasks.

The Quantum Privacy Network removes every structural barrier that previously made autonomous care navigation impossible.

## Personal Health Agents Operate Inside Quantum Privacy Cells

Personal Health Agents run within **Quantum Privacy Cells (QPCs)**—cryptographically bounded execution environments that ensure:

- PHI never leaves the Privacy Domain
- all actions follow role- and attribute-based Trust Criteria
- multi-party rights are enforced (patient, clinician, payer, caregiver, etc.)
- provenance and compliance are recorded as immutable Trust Blocks
- redisclosure rules (HIPAA, 42 CFR Part 2, GINA, state laws) are automatically enforced
- no external system can observe or interfere with the agent's reasoning

This creates the first safe environment in which AI can work directly with sensitive, real-world healthcare data.

## Capabilities of Personal Health Agents

Within QPN, Personal Health Agents can:

**Coordinate Clinical Workflows**

- schedule appointments
- route referrals
- pre-fill forms
- retrieve prior records
- trigger lab and imaging orders
- ensure clinical follow-up
- manage care-plan tasks

**Navigate Benefits and Costs**

- compute real-time co-pays and deductibles
- evaluate alternative treatment costs
- determine prior-authorization requirements
- surface affordability pathways
- recommend value-based care options
- adjust benefit design (via personalized plan design in Section 11.0)

**Manage Medications and Adherence**

- track fills, refills, and adherence
- coordinate pharmacy options
- initiate affordability programs
- escalate to clinicians when adherence drops
- integrate with pharmacogenomics (via Section 21.0)

**Coordinate Social and Community Support**

- connect patients with transportation, housing, food, mental-health, caregiver assistance
- integrate community resources (via Section 19.0)
- follow up when social barriers impede care

**Support Behavioral Health**

- monitor risk indicators
- provide nudges, prompts, or reminders
- escalate to crisis pathways when required
- integrate digital therapeutics

**Assist Caregivers and Families**

- share role-filtered information
- coordinate tasks
- send reminders
- enable secure two-way support

**Act as a Unified Patient Interface**

Patients no longer navigate portals—**the agent does it for them**, via the PPN.

## Personal Health Agents Use Dual-Use Infrastructure Without Detection

Because patients and clinicians already have lawful access to:

- payer portals
- PBM systems
- EHRs
- pharmacy systems
- lab portals
- community programs
- telehealth platforms

Personal Health Agents use these accounts through QPN as **dual-use infrastructure,** interacting via the Personal Privacy Networks of patients, clinicians, and caregivers, using existing apps and websites, and relying on their existing legal, regulatory, and contractual rights and access privileges.

To incumbents, each interaction appears as a normal patient or clinician request. Inside the QPN, these actions are part of a cryptographically governed, cross-organizational privacy-preserving care pathway.

No incumbent can block or detect the navigation agent's involvement without violating its obligations to the member or clinician.

This makes Personal Health Agents **unstoppable**, and able to ignore the immune system of entrenched incumbents that has historically blocked innovation and healthcare transformation.

## Autonomous Benefit & Affordability Optimization

Personal Health Agents can dynamically optimize out-of-pocket costs, treatment affordability, value-based alternatives, copay assistance, accumulator-proof affordability programs, EasyAccess Coupons (Section 10.6), employer or payer subsidies, and manufacturer incentives.

Agents can simulate and compare:

- pharmacies
- treatment modalities
- local provider pricing
- alternative care settings
- self-pay options
- DTC/DTP pricing

All without exposing PHI or financial data to manufacturers, PBMs, or other organizations.

## Safety, Oversight, and Governance for Personal Health Agents

Personal Health Agents are governed by:

- Adaptive Global Policy Weighting (AGPW)
- Human-Managed Trust Authorities (HTAs)
- jurisdiction-specific Trust Criteria
- auditability through Trust Blocks
- reversible, explainable lineage
- real-time safety constraints
- multi-stakeholder governance

AI agents cannot:

- exceed their role
- override clinical authority
- violate jurisdiction-specific laws
- disclose PHI
- perform biased or discriminatory actions

Personal Health Agents are safe, governable, and transparent.

## Personal Health Agents as Core Enablers of Personalized Healthcare

As described in Sections 1–19, the Quantum Privacy Network provides:

- unified evidence graphs
- care coordination
- benefit optimization
- affordability rails
- behavioral-health integration
- community support
- genomics and precision medicine
- federated real-world evidence
- continuous learning networks

Personal Health Agents bring these capabilities together into a **single, intelligent, lifelong companion** that helps each person navigate healthcare, benefits, prevention, and wellness.

## Conclusion

Personal Health Agents are not possible within legacy healthcare systems. They require:

- privacy-preserving computation
- cross-organizational workflow orchestration

- unified identity and consent
- cryptographically enforced governance
- zero-knowledge validation
- dual-use infrastructure
- reversible lineage and auditability

Only the Quantum Privacy Network provides the substrate for safe, equitable, autonomous care navigation.

Personal Health Agents will become the primary interface through which patients experience personalized healthcare—making the system more efficient, equitable, proactive, and human-centered than ever before.

---

# Patent Claims

---

## GROUP 1 — EasyAccess & PPN Onboarding (Claims 1–20)

### Family 1.1 — Personal Privacy Networks (PPNs) & QPC Governance

This family covers the core onboarding architecture enabling individuals, clinicians, and organizations to establish Personal Privacy Networks anchored in Quantum Privacy Cells. These claims define how data, identity, consent, and routing capabilities are assembled to create safe, compliant digital environments.

**Claim 1.** A system comprising, in any operable combination, one or more of:

**(a)** a Personal Privacy Network anchored by a Quantum Privacy Cell;

**(b)** a privacy-preserving data graph; a Proof-of-Trust enforcement layer;

**(c)** a relationship graph; a privacy-preserving routing engine; and

**(d)** an EasyAccess orchestration layer.

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 2.** The system of Claim 1, wherein **the routing engine enforces Trust Criteria inherited from all contributing resources.**

**Claim 3.** The system of Claim 1, wherein **the system prevents exposure of raw identifiers**.

**Claim 4.** **A method comprising**

**(a)** receiving health-related records**;**

**(b)** normalizing data;

**(c)** assigning Trust Criteria;

**(d)** generating a data graph.

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 5.** The method of Claim 4, wherein **record updates trigger workflow regeneration**.

**Claim 6.** A system comprising **a patient-facing workflow container comprising navigable components, consent policies, and decision-support elements**.

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 7.** The system of Claim 6, wherein **workflow components are dynamically updated based on clinical context.**

**Claim 8.** A system comprising **a provider-facing workflow container and verified treatment relationship validation.**

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 9.** A computer-readable medium storing instructions for **generating workflow threads linking multiple applications and enforcing privacy constraints.**

**Wherein** execution of the instructions causes the system to operate within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 10.** **A method comprising**

**(a)** validating identity;

**(b)** verifying treatment relationships;

**(c)** verifying consent;

**(d)** routing clinical records**.**

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 11.** The system of Claim 1 further comprising **multi-channel routing via SMS, fax, email, mobile messaging clients, Direct messaging, or EHR plug-ins.**

**Claim 12.** The system of Claim 1 wherein **workflow threads persist as immutable audit logs.**

## GROUP 2 — Clinical Workflows (Claims 21–50)

## Family 2.1 — Clinical Workflow Orchestration & Multi-App Care Journeys

This Claim Family describes systems and methods that orchestrate complex, multi-application clinical workflows using privacy-preserving routing, EasyAccess Threads, and QPC-governed safety constraints. These workflows link disparate apps, provider systems, EHRs, laboratory services, clinical decision support engines, and communication channels into unified care pathways.

The capabilities embodied here allow healthcare organizations to deliver fully integrated episodes of care, automate repetitive processes, reduce clinical friction, and ensure regulatory compliance.

**Licensing value:** This covers capabilities utilized by Epic, Cerner, athenahealth, telehealth platforms, clinical workflow vendors, and AI-driven orchestration systems.

**Claim 21.** A system comprising, in any operable combination, one or more of:

**(a) a clinical workflow engine**;

**(b) multi-application orchestration components**;

**(c) routing logic;** and

**(d) decision-support triggers** that update clinical threads based on patient status.

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 22.** The system of Claim 21 wherein **workflow steps include laboratory tests, imaging orders, procedures, referrals, or medication management.**

**Claim 23.** The system of Claim 21 wherein **the system enforces consent, identity verification, and regulatory compliance for each workflow step.**

**Claim 24.** **A method comprising**

**(a)** generating a clinical workflow thread;

**(b)** mapping tasks to appropriate providers or systems; and

**(c)** routing data or tasks.

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 25.** The method of Claim 24 wherein **workflow execution includes asynchronous task handling.**

**Claim 26.** The system of Claim 21 wherein **AI-based orchestration selects workflow components based on clinical guidelines.**

**Claim 27.** The system of Claim 21 comprises **multi-channel task delivery, including SMS, EHR plugins, fax, email, mobile messaging clients, Direct messaging, and app notifications.**

**Claim 28.** The system of Claim 21 wherein **clinical workflows adapt dynamically based on new clinical evidence.**

**Claim 29.** The system of Claim 21 wherein **tasks persist as immutable audit logs stored in Trust Blocks.**

**Claim 30.** A computer-readable medium storing instructions for **linking multiple clinical apps into a unified workflow.**

**Wherein** execution of the instructions causes the system to operate within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 31.** The computer-readable medium of Claim 30 wherein **workflow templates support reusable clinical care pathways.**

**Claim 32.** A system comprising **a provider-facing task dashboard integrating data from multiple workflows.**

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust

Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 33.** A method comprising **generating a longitudinal care thread combining events from multiple apps and provider systems.**

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 34.** The method of Claim 33 wherein **longitudinal threads are segmented into episodes of care.**

**Claim 35.** The system of Claim 21 wherein **clinical workflow orchestration includes real-time decision-support interventions.**

## Family 2.2 — Diagnostic, Laboratory & Genomic Ordering Workflows

This Claim Family defines privacy-preserving clinical workflows for diagnostic, laboratory, and genomic test ordering. These workflows include Complete Genomic Profiling (CGP), laboratory logistics, sample tracking, coverage verification, clinical indications analysis, and coordinated multi-stakeholder communication.

The invention enables seamless, automated diagnostic pathways across laboratories, EHRs, oncology systems, payers, and communication channels. Licensing value: CGP vendors, oncology decision-support companies, EHRs, lab networks (Quest, LabCorp), and genomic sequencing companies rely on these capabilities.

**Claim 36.** A system comprising, in any operable combination, one or more of:

**(a) diagnostic-order orchestration components;**

**(b) clinical-indications extraction;** and

**(c) automated routing** of laboratory tasks**.**

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 37.** The system of Claim 36 wherein **CGP ordering includes sample logistics and tracking.**

**Claim 38.** A method comprising

**(a) identifying clinical indications for laboratory testing;**

**(b) generating diagnostic workflow threads;** and

**(c) routing tasks to labs or clinicians.**

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 39.** The method of Claim 38 wherein **extracted indications include genomic, molecular, or pathology-derived features.**

**Claim 40.** The system of Claim 36 wherein **diagnostic workflows enforce payer coverage requirements.**

**Claim 41.** The system of Claim 36 wherein **sample handling events are recorded as immutable Trust Blocks.**

**Claim 42.** A computer-readable medium storing instructions to **extract pathology or genomic attributes for diagnostic recommendations.**

**Wherein** execution of the instructions causes the system to operate within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 43.** The computer-readable medium of Claim 42 wherein **extraction uses NLP/ML/AI models.**

**Claim 44.** A system comprising **a multi-stakeholder diagnostic dashboard for coordinating lab, clinician, and patient tasks.**

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 45.** The system of Claim 44 wherein **lab workflows include chain-of-custody verification.**

**Claim 46.** A system comprising **automated appeals generation for denied diagnostic tests.**

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 47.** The system of Claim 46 wherein **appeals bundles include structured clinical evidence.**

**Claim 48.** A method comprising **reconciling lab results with diagnostic recommendations.**

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 49.** The method of Claim 48 wherein **reconciliation triggers follow-up clinical tasks.**

**Claim 50.** The system of Claim 36 wherein **diagnostic workflows integrate with longitudinal care threads.**

## GROUP 3 — PRIOR AUTHORIZATION (CLAIMS 51–80)

### Family 3.1 — Quantum Privacy Cell-Governed Prior Authorization Engines

This Claim Family defines privacy-preserving prior authorization systems that evaluate payer rules, clinical guidelines, and coverage policies entirely within Quantum Privacy Cell (QPC) cleanrooms. These systems extract clinical attributes, analyze payer rules, and generate authorization decisions without exposing raw PHI. They enable automated, compliant, cross-organizational prior authorization workflows.

**Licensing value:** Every payer, prior-authorization vendor, clearinghouse, PBM, oncology platform, and automated utilization management system depends on these capabilities.

**Claim 51.** A system comprising, in any operable combination, one or more of:

**(a) a cleanroom;**

**(b) a payer-rules engine;**

**(c) a clinical evidence extraction layer;** and

**(d) a prior-authorization decision engine.**

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 52.** The system of Claim 51 wherein **payer rules include coverage criteria, medical-necessity policies, or benefit limitations.**

**Claim 53.** The system of Claim 51 wherein **extracted clinical attributes include diagnoses, lab results, imaging findings, or pathology-derived features.**

**Claim 54.** A method comprising **evaluating clinical data; applying payer rules; generating an authorization determination; and routing results.**

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 55.** The method of Claim 54 wherein **authorization decisions are updated dynamically when new evidence is added.**

**Claim 56.** The system of Claim 51 wherein **prior authorization workflows integrate with clinical workflows.**

**Claim 57.** The system of Claim 51 wherein **decisions persist as immutable Trust Blocks that may include decision rationale metadata, including provenance, evidence, or reasoning.**

**Claim 58.** A computer-readable medium **storing instructions to retrieve payer rules, evaluate clinical necessity, and generate decisions.**

**Wherein** execution of the instructions causes the system to operate within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 59.** The computer-readable medium of Claim 58 **wherein payer rules are represented as Trust Credentials.**

**Claim 60.** The system of Claim 51 wherein **decision rationale includes lineage metadata.**

**Claim 61.** A system comprising **a multi-stakeholder dashboard for real-time prior authorization status tracking.**

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 62.** The system of Claim 61 wherein **dashboard views differ for payers, providers, and patients.**

**Claim 63.** A method comprising **computing missing attributes required for authorization and generating tasks to collect them.**

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 64.** The method of Claim 63 wherein **missing attributes include clinical, demographic, financial, or coverage data.**

**Claim 65.** The system of Claim 51 **wherein authorization decisions integrate with downstream care-pathway tasks.**

## Family 3.2 — Clinical Necessity Extraction, Appeals & Verification

This Claim Family covers clinical-necessity extraction, automated appeals generation, and payer-verification workflows. These systems use NLP/NLU to extract clinical indicators, generate structured evidence bundles, reconcile payer responses, and support automated appeals.

**Licensing value:** Payers, EHRs, utilization management vendors, oncology clinical-decision-support tools, and AI/ML data extraction vendors all rely on these operations—making this a high-leverage IP category.

**Claim 66.** A system comprising, in any operable combination, one or more of:

**(a) a clinical-indications extraction engine;**

**(b) an appeals-generation module;** and

**(c) a payer-response reconciliation engine.**

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 67.** The system of Claim 66 wherein **extracted indicators include genomic markers, pathology-derived features, or lab values.**

**Claim 68.** The system of Claim 66 wherein **extracted evidence is validated using PoT-governed provenance metadata.**

**Claim 69.** **A method comprising**

**(a)** extracting clinical attributes;

**(b)** generating structured appeals templates;

**(c)** submitting appeals, and

**(d)** reconciling payer responses.

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 70.** The method of Claim 69 wherein **appeals bundles include treatment alternatives.**

**Claim 71.** A computer-readable medium storing instructions for **automated extraction of clinical necessity criteria.**

**Wherein** execution of the instructions causes the system to operate within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 72.** The CRM of Claim 71 wherein **extraction uses NLP, ML, or pattern-recognition models.**

**Claim 73.** A system comprising **a multi-channel appeals routing engine.**

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 74.** The system of Claim 73 wherein **routing includes Direct messaging, email, mobile messaging clients, fax, EHR plugins, or portal submission.**

**Claim 75.** A system comprising **real-time payer-response reconciliation.**

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 76.** The system of Claim 75 **wherein reconciliation updates evidence graphs.**

**Claim 77.** A method comprising **generating missing-information tasks for appeals submission.**

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 78.** The method of Claim 77 wherein **tasks include requests to patients, providers, or labs.**

**Claim 79.** A system comprising **automated appeals escalation workflows.**

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 80.** The system of Claim 79 wherein **escalation depends on payer timing or regulatory deadlines.**

## GROUP 4 — Patient Assistance & Benefits Optimization (Claims 81–110)

### Family 4.1 — Tokenized Patient Assistance Eligibility Engines

This Claim Family defines privacy-preserving architectures for determining patient eligibility for manufacturer-, payer-, or philanthropic-sponsored financial assistance programs. These systems evaluate clinical, financial, demographic, and coverage criteria entirely within QPC-governed computational domains, ensuring that sensitive information is never exposed outside authorized contexts.

**Licensing value**: All patient-assistance vendors, PBMs, pharma hubs, affordability platforms, manufacturer copay programs, and payer, or Third-Party-Administrator eligibility systems depend on these capabilities.

**Claim 81.** A system comprising, in any operable combination, one or more of:

**(a)** an eligibility engine;

**(b)** a financial-attribute evaluation layer;

**(c)** a clinical-criteria evaluator; and

**(d)** a Patient Assistance Eligibility Token generator.

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 82.** The system of Claim 81 wherein **income verification includes patient-uploaded documentation processed within the system.**

**Claim 83.** The system of Claim 81 wherein **eligibility tokens encode multi-stakeholder usage and revocation constraints.**

**Claim 84.** A method comprising receiving **demographic, clinical, and financial data; validating attributes; computing eligibility; and issuing a trust-verified eligibility token.**

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 85.** The method of Claim 84 wherein **eligibility computations incorporate coverage or benefit rules.**

**Claim 86.** The system of Claim 81 wherein **eligibility tokens persist as immutable Trust Blocks.**

**Claim 87.** A computer-readable medium storing instructions **for multi-dimensional eligibility evaluation.**

**Wherein** execution of the instructions causes the system to operate within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 88.** The CRM of Claim 87 wherein **eligibility criteria include regulatory, contractual, or payer-specific requirements.**

**Claim 89.** The system of Claim 81 comprising **multi-channel routing of eligibility results.**

**Claim 90.** The system of Claim 89 wherein **routing includes SMS, email, mobile messaging clients, EHR plugins, or mobile apps.**

**Claim 91.** A method comprising **evaluating eligibility using clinical attributes.**

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 92.** The method of Claim 91 wherein **attributes include diagnoses, lab results, or genomic findings.**

**Claim 93.** A system comprising **automated renewal or re-certification workflows for patient-assistance programs.**

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 94.** A system comprising **income and coverage re-verification triggered by time-based or event-based rules.**

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 95.** The system of Claim 81 wherein **eligibility workflows integrate with prior authorization, benefit verification, or coverage-determination workflows.**

## Family 4.2 — Virtual Debit Cards, Accumulator Protection & Rebate Settlement

This Claim Family covers workflows for issuing virtual debit cards, applying co-pay credits, preventing accumulator and maximizer diversion, and reconciling pharmacy and payer claims. These systems allow pharmacy and patient payments to occur outside NCPDP rails while retaining full compliance and trust-verified auditing.

**Licensing value:** PBMs, co-pay card vendors, affordability platforms, fintech health-payment systems, pharma manufacturers, and specialty pharmacies all require these protected payment and settlement processes.

**Claim 96.** A system comprising, in any operable combination, one or more of:

**(a)** a **virtual debit-card generator**;

**(b)** a **payment authorization engine**; and

**(c)** a **non-NCPDP co-pay processing rail**.

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 97.** The system of Claim 96 wherein **debit-card numbers are single-use or dynamically regenerated.**

**Claim 98.** The system of Claim 96 wherein **accumulator protection includes suppressing payer-visible claim identifiers.**

**Claim 99.** A method comprising **issuing virtual cards; authorizing payments; and applying credits to patient balances.**

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 100.** The method of Claim 99 wherein **payment authorization adapts to payer rules.**

**Claim 101.** A system comprising **rebate-reconciliation engines validating pharmacy EOBs.**

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 102.** The system of Claim 101 wherein **rebates are applied to outstanding debit-card balances.**

**Claim 103.** A computer-readable medium storing instructions to **reconcile pharmacy payments with rebate authorizations.**

**Wherein** execution of the instructions causes the system to operate within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 104.** The CRM of Claim 103 wherein **reconciliation updates evidence graphs.**

**Claim 105.** A system comprising **multi-channel routing of benefits and rebate notifications.**

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 106.** The system of Claim 105 wherein **routing includes SMS, email, mobile messaging clients, or app notifications.**

**Claim 107.** A method comprising **computing accumulator exposure and applying safeguards.**

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 108.** The method of Claim 107 wherein **safeguards include redirecting payments away from NCPDP rails.**

**Claim 109.** A system comprising **a multi-party funding network for patient-assistance disbursements.**

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 110.** The system of Claim 109 wherein **funding sources include manufacturers, payers, or philanthropic entities.**

## GROUP 5 — Plan Design, Cost-Sharing & Value-Based Incentives (Claims 111–130)

### Family 5.1 — Personalized Plan Design & Dynamic Benefit Adjustment

This Claim Family defines personalized insurance plan design engines driven by trust-verified clinical and behavioral evidence graphs. These systems dynamically adjust coverage tiers, co-pays, deductibles, and network eligibility to optimize financial protection and encourage high-value care.

**Licensing value:** National payers, PBMs, employer health plans, value-based care platforms, actuarial vendors, self-ensured employers, and digital benefits platforms must license these capabilities.

**Claim 111.** A system comprising, in any operable combination, one or more of:

**(a)** an **evidence graph**;

**(b)** a **plan-design engine**; and

**(c)** a **personalization engine** adjusting coverage or cost-sharing.

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 112.** The system of Claim 111 wherein **plan updates incorporate patient-preference models.**

**Claim 113.** A method comprising **retrieving evidence; computing risk or value metrics; and adjusting benefit design parameters.**

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 114.** The method of Claim 113 wherein **plan design updates occur in real time.**

**Claim 115.** A system comprising **dynamic adjustment of co-pays and deductibles based on value signals.**

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 116.** The system of Claim 115 **wherein adjustments depend on adherence or outcome metrics.**

**Claim 117.** A computer-readable medium storing **instructions for computing plan-design updates.**

**Wherein** execution of the instructions causes the system to operate within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 118.** The CRM of Claim 117 wherein **actuarial inputs incorporate trust-verified outcomes.**

**Claim 119.** A system comprising **a patient-facing benefits interface showing updated coverage.**

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 120.** The system of Claim 119 wherein **notifications include SMS, app, or portal messaging.**

## Family 5.2 — Value-Based Provider Ranking & Incentive Models

This Claim Family covers provider ranking, referral optimization, and incentive distribution based on value, quality, cost-effectiveness, and patient-preference attributes. These mechanisms allow plans to steer care to the highest-value clinicians and facilities.

**Licensing value:** Payers, large provider networks, referral platforms, value-based insurance designs, and quality-measurement companies all rely on these structures.

**Claim 121.** A system comprising, in any operable combination, one or more of:

**(a)** a **provider-ranking engine**;

**(b)** a **value-scoring module**; and

**(c) referral optimization logic**.

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 122.** The system of Claim 121 wherein **ranking includes quality, safety, or cost measures.**

**Claim 123.** A method comprising **computing provider value scores and routing referrals accordingly.**

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 124.** The method of Claim 123 **wherein referral routing incorporates patient preferences.**

**Claim 125.** A system comprising **tokenized incentives for high-value provider or patient behavior.**

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 126.** The system of Claim 125 wherein **incentives include premium reductions or reward credits.**

**Claim 127.** A computer-readable medium storing instructions **to compute multi-stakeholder value alignment.**

**Wherein** execution of the instructions causes the system to operate within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 128.** The CRM of Claim 127 wherein **incentive weights depend on clinical outcomes.**

**Claim 129.** A system comprising **plan adjustments driven by provider performance metrics.**

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust

Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 130.** The system of Claim 129 wherein **performance metrics update evidence graphs.**

## GROUP 6 — Population Health, Public Health & Clinical Research (Claims 131–150)

### Family 6.1 — Public Health Surveillance & Zero-Knowledge Population Analytics

This Claim Family defines privacy-preserving, population-scale analytic engines that compute public health, epidemiological, and biosurveillance metrics inside Quantum Privacy Cells (QPCs). These systems ingest multi-source clinical, claims, genomic, laboratory, vaccination, and social-determinant datasets, and compute population-level outputs without exposing individual-level information.

**Licensing value:** Governments, research networks, CDC/NIH/WHO-aligned analytics vendors, academic medical centers, RWE platforms, and pharmacovigilance vendors all require these capabilities.

**Claim 131.** A system comprising, in any operable combination, one or more of:

**(a)** a **public-health cleanroom**;

**(b) multi-source PPN data ingestion**; and

**(c) epidemiological metric computation**.

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 132.** The system of Claim 131 wherein **outputs include outbreak detection, anomaly identification, or cluster analysis.**

**Claim 133.** A method comprising **ingesting population-health data; performing cleanroom analytics; and releasing aggregate outputs without revealing PHI.**

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 134.** The system of Claim 131 wherein **analytic parameters include variant tracking or genomic surveillance.**

**Claim 135.** A computer-readable medium storing instructions **for computing epidemiological indicators.**

**Wherein** execution of the instructions causes the system to operate within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 136.** The CRM of Claim 135 wherein **indicators include R-number, positivity rates, or transmission curves.**

**Claim 137.** A system comprising **a multi-stakeholder public-health dashboard updated from cleanroom analytics.**

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 138.** The system of Claim 137 wherein **access is restricted by jurisdiction-specific Trust Criteria.**

**Claim 139.** A method comprising **computing geospatial public-health signals and routing alerts to authorized agencies.**

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 140.** The method of Claim 139 wherein **alerts are delivered via SMS, email, or authenticated API endpoints.**

### Family 6.2 — Clinical Research, CRAACO & Zero-Knowledge Trial Matching

This Claim Family includes privacy-preserving clinical research orchestration and Clinical Research As A Care Option (CRAACO) workflows. These systems automatically detect trial eligibility, generate patient- and provider-facing research threads, perform zero-knowledge trial matching, manage consent workflows, and route research tasks across decentralized sites.

**Licensing value**: CROs, pharma sponsors, decentralized clinical trial vendors, academic research organizations, and oncology precision-medicine platforms all rely on these capabilities.

**Claim 141.** A system comprising, in any operable combination, one or more of:

**(a)** a **research-eligibility engine**;

**(b)** a **clinical-indications analysis engine**; and

**(c) trial-matching modules**.

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 142.** The system of Claim 141 wherein **eligibility detection uses clinical, genomic, or molecular attributes.**

**Claim 143.** A method comprising **identifying research opportunities; generating patient-facing research threads; and collecting consent.**

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 144.** The method of Claim 143 wherein **consent is revocable and persists as immutable Trust Blocks.**

**Claim 145.** A computer-readable medium storing instructions for **zero-knowledge mapping of patient attributes to trial eligibility rules.**

**Wherein** execution of the instructions causes the system to operate within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 146.** The CRM of Claim 145 wherein **eligibility mappings exclude direct exposure of PHI to sponsors.**

**Claim 147.** A system comprising **a decentralized research-task routing engine.**

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 148.** The system of Claim 147 wherein **routing includes sample logistics, remote tasks, or telehealth investigator visits.**

**Claim 149.** A method comprising **generating investigator, coordinator, or sponsor tasks from research threads.**

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 150.** The method of Claim 149 wherein **research tasks integrate with population-health evidence graphs.**

## GROUP 7 — PNX Marketplace, Tokens & Multi-Sided Exchange (Claims 151–160)

### Family 7.1 — Marketplace Architecture, Resource Tokens & Exchange Tokens

This Claim Family defines the Privacy Network Exchange (PNX), a multi-sided marketplace where data, services, AI models, workflows, identities, and digital resources are tokenized and exchanged under QPC-governed privacy and Proof-of-Trust guarantees. Resource Tokens encode rights, obligations, and provenance for contributed assets, while Exchange Tokens allocate fractional value from marketplace activity.

**Licensing value:** Hyperscalers (AWS, Azure, Google Cloud), enterprise SaaS vendors, payment networks, identity providers, app ecosystems, AI platforms, telecoms, and global exchange operators must license these foundational marketplace and tokenomics structures.

**Claim 151.** A system comprising, in any operable combination, one or more of:

**(a)** a multi-sided **Privacy Network Exchange**;

**(b)** a **resource-tokenization engine**; and

**(c)** a **value-sharing layer**.

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 152.** The system of Claim 151 wherein **resource tokens encode rights to data, models, workflows, verified identities, digital services, user engagement, contractual rights, computation, regulatory rights, consents, and other resources.**

**Claim 153.** The system of Claim 151 **wherein exchange tokens allocate fractional rights to marketplace value.**

**Claim 154.** A method comprising **receiving digital resources; assigning Trust Criteria; tokenizing the resources; and routing them to authorized participants.**

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 155.** The method of Claim 154 wherein **value distribution uses contribution-weighted attribution scores.**

**Claim 156.** A computer-readable medium storing instructions to **enroll third-party vendors and wrap their functions as EasyAccess components.**

**Wherein** execution of the instructions causes the system to operate within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 157.** The CRM of Claim 156 wherein **components are sandboxed within a QPN-bounded execution environment.**

**Claim 158.** A system comprising **liquidity pools funding marketplace operations, and resource-token staking.**

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 159.** The system of Claim 158 wherein **staked tokens yield governance or economic rights.**

**Claim 160.** A system comprising **AI-driven optimization engines recommending resource combinations, vendors, or flows.**

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

## GROUP 8 —Direct Contracting & Ecosystem Optimization (Claims 161–175)

### Family 8.1 — Direct-to-Patient & Direct-to-Employer Manufacturer Contracting

This family covers QPN-enabled contracting models where manufacturers interact directly with patients, employers, caregivers, or clinicians using privacy-preserving workflow

threads. Adaptive treatment access, dynamic pricing, safety gating, and incentive alignment occur inside QPCs using clinical, behavioral, and contextual signals without exposing PHI to payers or PBMs.

**Licensing Value:** Strategic, high-value coverage for pharmaceutical, device, diagnostic, and digital-therapeutic manufacturers seeking direct contracting models. Applies to drug pricing engines, metabolic-health vendors, REMS-linked access platforms, and employer contracting ecosystems.

**Claim 161.** A system comprising, in any operable combination, one or more of:

**(a) adaptive manufacturer–patient contracting engines** configured to compute real-time treatment pricing or therapeutic access based on verified clinical, behavioral, or contextual indicators;

(**b) privacy-preserving workflow threads** enforcing safety, affordability, or benefit-alignment constraints; and

**(c) dynamic incentive-alignment mechanisms** generating personalized support, rebates, or adherence-linked adjustments without exposing PHI to intermediaries.

**Wherein** the system executes within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 162.** A method for enabling **direct manufacturer contracting comprising:**

**(a)** receiving zero-knowledge eligibility or risk indicators from a patient;

**(b)** determining personalized access, pricing, incentives, or routing options;

**(c)** enforcing therapeutic-specific Trust Criteria; and

**(d)** executing the contracting transaction without exposing clinical, behavioral, or contextual signals to external entities.

**Wherein** the method executes within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 163.** A computer-readable medium storing instructions that, when executed, **cause a system to perform manufacturer–patient or manufacturer–employer contracting using verified eligibility, incentive, safety, and benefit logic without revealing underlying clinical, behavioral, or contextual signals.**

**Wherein** execution of the instructions causes the system to operate within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

## Family 8.2 — PBM-Resistant, Zero-Knowledge Price & Benefit Adjudication

This family covers real-time drug and benefit adjudication where accumulators, formulary rules, affordability logic, and pricing are computed with zero-knowledge protection, preventing PBMs or payers from manipulating, blocking, or surveilling transactions.

**Licensing Value:** Targets PBMs, payers, discount-card ecosystems, benefits platforms, and drug-pricing engines — extremely high strategic value.

**Claim 164.** A system comprising, in any operable combination, one or more of:

(a) **zero-knowledge adjudication engines** configured to compute therapeutic pricing, rebates, affordability logic, or accumulator outcomes;

(b) **privacy-bounded benefit-routing mechanisms** that prevent intermediaries from blocking, reordering, or modifying workflows; and

(c) **compliance evaluators** ensuring adherence to clinical, labeling, or formulary constraints without revealing PHI.

**Wherein** the system executes within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 165.** **A method for PBM-resistant therapeutic adjudication comprising**:

**(a)** obtaining eligibility or affordability indicators;

**(b)** executing pricing, accumulator, or compliance calculations in zero-knowledge form; and

**(c)** returning patient-facing affordability outputs without exposing clinical, behavioral, or lifestyle context to any intermediary.

**Wherein** the method executes within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 166.** A computer-readable medium storing instructions for **performing zero-knowledge therapeutic adjudication using privacy-bounded outputs as inputs to downstream routing, incentive, or pricing workflows.**

**Wherein** execution of the instructions causes the system to operate within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

## Family 8.3 — Direct Manufacturer–Employer Wellness & Population Optimization

This family covers QPN-enabled agreements between manufacturers and employers (or employer coalitions) using distributed lifestyle-signal graphs to generate adaptive incentives, pricing paths, adherence gating, and productivity-linked optimization.

**Licensing Value:** High applicability to employer wellness platforms, GLP-1 optimization vendors, metabolic-health ecosystems, and population-health contracting infrastructure.

**Claim 167.** A system comprising, in any operable combination, one or more of:

**(a) employer-aligned optimization engines** configured to produce population-scaled incentives, pricing adjustments, or adherence-linked routing using federated lifestyle-signal graphs;

**(b) privacy-preserving performance evaluators** generating zero-knowledge outcome predictions; and

**(c) cross-sector routing mechanisms** enabling manufacturer-funded wellness or therapeutic support without disclosing PHI.

**Wherein** the system executes within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 168.** **A method for population-optimized manufacturer–employer contracting** comprising:

**(a) ingesting encrypted engagement or lifestyle signals**;

**(b) computing zero-knowledge outcome trajectories**; and

**(c) applying environment-adaptive incentives or care pathways**.

**Wherein** the method executes within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 169.** A computer-readable medium storing instructions for **executing employer-aligned therapeutic optimization workflows using privacy-bounded behavioral, environmental, or clinical indicators.**

**Wherein** execution of the instructions causes the system to operate within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

## Family 8.4 — Tokenized Fulfillment, Serialized Dispensing & REMS Compliance

This family covers REMS-regulated dispensing, serialized fulfillment, adverse-event gating, and safety thresholds enforced within the QPN. Trust Blocks encode lineage to guarantee compliance without exposing sensitive information.

**Licensing Value:** Critical for REMS platforms, specialty pharmacies, controlled-substance systems, and high-risk therapeutic ecosystems.

**Claim 170.** A system comprising, in any operable combination, one or more of:

**(a) tokenized therapeutic-fulfillment engines** applying REMS, labeling, or safety constraints;

**(b) serialization engines generating dispense-event tokens**; and

**(c) routing mechanisms directing fulfillment tokens to authorized dispensers** while preventing visibility into PHI by any intermediary.

**Wherein** the system executes within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 171.** **A method for privacy-preserving therapeutic fulfillment** comprising:

**(a)** verifying safety thresholds;

**(b)** generating a fulfillment token;

**(c)** routing the token to authorized dispensing entities; and

**(d)** storing immutable dispensing lineage.

**Wherein** the method executes within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 172.** A computer-readable medium storing instructions for **performing zero-knowledge REMS compliance, serialized therapeutic dispensing, or tokenized access workflows.**

**Wherein** execution of the instructions causes the system to operate within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

## GROUP 9 — EasyAccess Coupons, Adaptive Incentives & Cross-Economy Engagement (Claims 176–185)

### Family 9.1 — EasyAccess Reward Incentives & Zero-Knowledge Coupons

This family covers QPN-enabled incentive and coupon systems that generate, route, validate, and redeem value without revealing eligibility conditions, PHI, or behavioral information.

**Licensing Value:** Applies to food-delivery platforms, manufacturers, e-commerce systems, employers, digital-health apps, and benefits programs.

**Claim 176.** A system comprising, in any operable combination, one or more of:

**(a)** zero-knowledge incentive engines generating electronic coupons based on verified eligibility, behavioral, or environmental context;

**(b)** privacy-preserving redemption mechanisms; and

**(c)** fraud-resistant lineage tracking.

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 177.** **A method for issuing privacy-preserving incentives** comprising:

**(a)** deriving eligibility indicators;

**(b)** generating a privacy-bounded coupon or rebate; and

**(c)** enabling redemption without exposing underlying clinical, behavioral, or financial information.

**Wherein** the method operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 178.** A computer-readable medium storing instructions for **managing zero-knowledge coupons, incentives, or rebates using verified eligibility and fraud-resistant lineage.**

**Wherein** execution of the instructions causes the system to operate within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

## Family 9.2 — Environment-Adaptive Nudging & Healthy Defaults

This family covers adaptive nudging systems that interact with e-commerce, delivery, media, transportation, and financial platforms using zero-knowledge personalization from PPNs.

**Licensing Value:** High-value claims for major consumer-online ecosystems and device OEMs.

**Claim 179.** A system comprising, in any operable combination, one or more of:

**(a) environment-adaptive personalization engines** adjusting search results, recommendations, or default options using QPC-computed signals;

**(b) zero-knowledge interaction modules** exchanging personalization outputs with external services; and

**(c) privacy-bounded behavioral reinforcement mechanisms**.

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 180:** **A method for generating healthy default pathways** comprising:

**(a)** computing verified risk or preference indicators;

**(b)** conducting zero-knowledge exchanges with external services; and

**(c)** adjusting outputs to reinforce beneficial behaviors.

**Wherein** the method operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 181.** A computer-readable medium storing instructions for **applying cross-sector nudging logic using privacy-preserving behavioral, environmental, or lifestyle indicators computed inside QPCs.**

**Wherein** execution of the instructions causes the system to operate within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

## Family 9.3 — Federated Behavioral-Signal Integration & Risk-Adaptive Incentives

This family covers the creation of federated lifestyle-signal graphs and the generation of risk-adaptive incentives that remain entirely within the Quantum Privacy Network.

**Licensing Value:** Applies to digital-therapeutic ecosystems, metabolic-health vendors, mental-health platforms, and employer wellness programs.

**Claim 182.** A system comprising, in any operable combination, one or more of:

**(a) federated lifestyle-graph engines** computing behavioral, environmental, caregiver, or device-derived signals;

**(b) zero-knowledge risk-indicator generators** producing incentive inputs; and

**(c) adaptive routing mechanisms** forwarding privacy-bounded outputs to authorized services.

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 183.** **A method comprising:**

**(a)** ingesting encrypted lifestyle signals;

**(b)** computing privacy-bounded risk trajectories; and

**(c)** generating incentives or warnings without revealing underlying behavioral, clinical, or contextual signals.

**Wherein** the method operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 184.** A computer-readable medium storing instructions for **performing federated lifestyle-graph computation and producing privacy-bounded outputs consumable by external systems.**

**Wherein** execution of the instructions causes the system to operate within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

## Family 9.4 — Multi-Sponsor Funding, Fraud-Resistant Redemption & Cross-Economy Routing

This family covers multi-sponsor cost-sharing, routing, and value allocation across manufacturers, employers, payers, community organizations, and government programs.

**Licensing Value:** Essential coverage for all coupon/incentive ecosystems and multi-payer subsidy models.

**Claim 185.** A system comprising, in any operable combination, one or more of:

**(a) multi-sponsor incentive-routing engines** allocating value across manufacturers, employers, payers, or public programs using verified lineage;

**(b) fraud-resistant redemption logic** executing in zero-knowledge form; and

**(c) cross-sector workflow threads** enabling compliant distribution of multi-party incentive contributions.

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

## GROUP 10 — CROSS-SECTOR, DUAL-USE PERSONALIZATION & BEHAVIORAL OPTIMIZATION (Claims 186–200)

### Family 10.1 — Privacy-Preserving Cross-Sector Personalization Threads

This family covers core QPN mechanisms for cross-sector personalization, enabling a Personal Privacy Network (PPN) to interact with e-commerce, financial services, entertainment, workplace, and transportation ecosystems using zero-knowledge signals. All personalization logic executes inside the user's QPC-bounded Privacy Domain, ensuring external systems receive minimal-disclosure eligibility or personalization outcomes without learning behavioral, health, or contextual data. These capabilities underpin privacy-preserving personalization, behavioral-health optimization, contextual nudging, and distributed incentive delivery across the broader economy.

**Licensing Value:** High commercial relevance for Amazon, Apple, Google, Meta, TikTok, Netflix, Walmart, Instacart, Uber, DoorDash, Shopify, Stripe, PayPal, financial platforms, and device OEMs implementing personalization, recommendation engines, ranking logic, or behavior-adaptive interfaces.

**Claim 186.** A system comprising, in any operable combination, one or more of:

**(a)** a **Personal Privacy Network** (PPN) comprising Quantum Privacy Cells (QPCs) maintaining an encrypted, provenance-bound engagement graph representing behavioral, contextual, environmental, or preference signals;

**(b)** a **dual-use cross-sector interaction engine** configured to initiate privacy-preserving zero-knowledge interactions with external services across e-commerce, financial, consumer-online, entertainment, workplace, or transportation ecosystems;

**(c)** a **Trust-Criteria evaluation layer** configured to generate privacy-bounded personalization outputs based on multi-party constraints contributed by clinicians, caregivers, employers, public-health entities, or the individual; and

**(d)** a **routing engine** configured to deliver minimal-disclosure eligibility, personalization, or incentive signals to external systems without revealing underlying health or behavioral information.

**Wherein** the system executes within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 187.** The system of Claim 186 **wherein zero-knowledge interactions provide external systems only a binary or categorical result indicating eligibility, relevance, or personalization tier without exposing behavioral, lifestyle, health, or risk-sensitive data.**

**Claim 188.** The system of Claim 186 **wherein multi-party Trust Criteria comprise constraints derived from regulatory rules, clinical guidance, safety thresholds, employer policies, parental or guardian authorization, or user-defined controls.**

**Claim 189.** The system of Claim 186 **wherein the personalized output comprises at least one of: tailored ranking of digital content, dynamic ordering of food or retail options, real-time environmental-risk adjustments, or adaptive filtering of harmful digital content.**

**Claim 190.** The system of Claim 186 **wherein all personalization logic executes entirely within the individual's QPC-bounded Privacy Domain, preventing external entities from learning or inferring PHI, behavioral trajectories, or risk indicators.**

## Family 10.2 — Dual-Use Cross-Sector Infrastructure Integration

This family describes the QPN capability of reusing existing digital infrastructures—e-commerce catalogs, search engines, payment processors, financial-wellness tools, entertainment platforms, and workplace systems—as dual-use personalization resources for health-linked optimization. The integration occurs via zero-knowledge exchanges and does not require external systems to modify APIs or accept new data. QPCs privately fuse contextual metadata with health-linked Trust Criteria to produce personalization or incentive outputs that remain fully privacy-bounded.

**Licensing Value:** Broad applicability for Amazon, Google, Walmart, PayPal, Visa, Mastercard, Shopify, Square, device platforms, operating systems, and any personalization engine seeking compliant health-linked optimization.

**Claim 191.** **A method comprising**:

**(a)** interfacing a PPN with external digital-commerce, financial-services, consumer-online, or entertainment platforms via zero-knowledge access protocols;

**(b)** acquiring contextual metadata without sharing PHI;

**(c)** combining such metadata with internal Trust Criteria; and

**(d)** generating privacy-bounded personalization or incentive outputs;

**Wherein** all computations occur within QPCs under cryptographic constraint enforcement within a QPN-enabled infrastructure comprising at least one of: QPCs, Privacy Domains, Trust Criteria, PoT, Trust Blocks, or EasyAccess workflow threads.

**Claim 192.** The method of Claim 191 wherein **contextual metadata includes at least one of: nutritional attributes, product classifications, pricing, environmental risk factors, engagement categories, or financial-stress indicators.**

**Claim 193.** The method of Claim 191 wherein **dual-use integration reuses existing accounts, permissions, or rights possessed by patients, clinicians, caregivers, or employers to execute health-relevant computations without requiring modification to the external system.**

**Claim 194.** The method of Claim 191 wherein **the external system receives no persistent identifiers, device-level identifiers, account-linked metadata, or health-correlated behavioral indicators.**

### Family 10.3 — Distributed Value-Aligned Nudging & Incentive Delivery

This family covers distributed incentive delivery and nudging workflows that operate across multiple external ecosystems using QPC-verified signals. These systems enable real-time health-aligned behavior shaping, including healthy defaults, context-aware ordering, risk-adaptive suppression, and micro-interventions triggered by QPC-verified signals—all without revealing underlying lifestyle or health data.

**Licensing Value:** Extremely high value for behavioral-health platforms, metabolic-health vendors, GLP-1 optimization engines, wellness programs, digital therapeutics, e-commerce platforms, media companies, and employer or insurer incentive ecosystems.

**Claim 195.** A system comprising, in any operable combination, one or more of:

**(a)** an **incentive-orchestration engine**, configured to deliver distributed value-aligned nudges across digital ecosystems;

**(b) healthy defaults, context-aware EasyAccess benefits**, risk-adaptive suppression of harmful offerings, or micro-interventions triggered by verified criteria; and

**(c) privacy-bounded routing logic** ensuring that only minimal-disclosure outputs reach external systems.

**Wherein** the system executes within a QPN-enabled infrastructure comprising at least one of: QPCs, Privacy Domains, Trust Criteria, PoT, Trust Blocks, or EasyAccess workflow threads.

**Claim 196.** The system of Claim 195 wherein **micro-interventions include stress-reduction prompts, sleep-stability recommendations, hydration or movement reminders, caregiver alerts, or behavioral-risk warnings.**

**Claim 197.** The system of Claim 195 wherein **incentive delivery is tied to zero-knowledge eligibility tests confirming alignment with clinical appropriateness, risk status, or supervised-care pathways.**

**Claim 198.** The system of Claim 195 wherein **incentives are funded by manufacturers, employers, health plans, public-health agencies, community organizations, philanthropic sponsors, or individuals.**

**Claim 199.** The system of Claim 195 wherein **nudges are dynamically adjusted based on time-of-day context, environmental conditions, user stress indicators, or caregiver-linked constraints.**

**Claim 200.** The system of Claim 195 wherein **no external system can determine the clinical rationale, health status, behavioral indication, or risk factor underlying any nudge, incentive, or recommendation.**

## GROUP 11 — LIFESTYLE-SIGNAL–DRIVEN, ADAPTIVE HEALTH OPTIMIZATION (Claims 201–220)

### Family 11.1 — Federated Lifestyle-Signal Graphs

This family covers the construction and continuous recomputation of lifestyle-signal graphs, incorporating device telemetry, movement patterns, food choices, media consumption, mobility, behavioral engagement, stress indicators, and social signals. Performs analysis and generate privacy-bounded outputs for use in clinical care, benefit logic, employer workflows, digital therapeutics, and population-health systems.

**Licensing Value:** Applies broadly to digital therapeutics, metabolic platforms, GLP-1 optimization vendors, mental-health tools, chronic-care platforms, and any system using lifestyle-derived risk trajectories.

**Claim 201.** A system comprising, in any operable combination, one or more of:

**(a) mechanism configured to generate and maintain a federated lifestyle-signal graph** representing encrypted behavioral, environmental, social, nutritional, mobility, media-consumption, or device-telemetry signals;

**(b) processing logic** computing indicators of risk, resilience, stability, or clinical relevance; and

**(c)** a **distributed output engine** generating privacy-bounded signals for authorized stakeholders.

**Wherein** the system executes within a QPN-enabled infrastructure comprising at least one of: QPCs, Privacy Domains, Trust Criteria, PoT, Trust Blocks, or EasyAccess workflow threads.

**Claim 202.** The system of Claim 201 wherein **lifestyle signals are tagged with cryptographically verifiable provenance attributes, jurisdictional flags, or multi-party lineage constraints.**

**Claim 203.** The system of Claim 201 wherein the **lifestyle-signal graph is continuously recomputed based on encrypted real-time inputs from authorized stakeholders or devices.**

**Claim 204.** The system of Claim 201 wherein **the lifestyle-signal graph is used to generate zero-knowledge outputs including risk markers, trajectory projections, eligibility results, or personalized plan modifications.**

**Claim 205.** The system of Claim 201 wherein **lifestyle-signal processing includes stability analysis, anomaly detection, stress-load modeling, environmental-risk modeling, sedentary-behavior detection, or nutritional-exposure modeling.**

**Claim 206.** The system of Claim 201 wherein **lifestyle signals are never centralized or pooled across users, and only privacy-bounded outputs are shared.**

## Family 11.2 — Environment-Adaptive Intervention Logic

This family covers QPC-executed environment-adaptive interventions triggered by lifestyle-signal trajectories and contextual risk indicators. All computation occurs inside the user's Privacy Domain, enabling personalized defaults, dynamic filtering, adaptive recommendations, and real-time risk mitigation across connected ecosystems.

**Licensing Value.** High strategic relevance for behavioral-health systems, digital therapeutics, employer wellness, public-health surveillance, consumer apps, OS-level personalization engines, and environmental-exposure platforms.

**Claim 207.** **A method comprising**:

**(a)** detecting environment-relevant behavioral or physiological patterns within QPCs;

**(b)** evaluating said patterns under multi-party Trust Criteria;

**(c)** determining whether intervention criteria are satisfied; and

**(d)** triggering context-appropriate interventions across digital ecosystems in zero-knowledge form.

**Wherein** the method executes within a QPN-enabled infrastructure comprising at least one of: QPCs, Privacy Domains, Trust Criteria, PoT, Trust Blocks, or EasyAccess workflow threads.

**Claim 208.** The method of Claim 207 wherein **the interventions comprise at least one of: personalized defaults, dynamic content filtering, retail-level recommendation adjustments, or context-aligned EasyAccess incentives.**

**Claim 209.** The method of Claim 207 wherein **threshold values for triggering interventions are jointly contributed by clinicians, caregivers, employers, public-health authorities, or the user.**

**Claim 210.** The method of Claim 207 wherein **intervention intensity, incentive structure, or recommendation modality is adjusted based on real-time environmental exposure, mobility context, stress-trajectory indicators, or device-derived patterns.**

**Claim 211.** The method of Claim 207 wherein **all interventions enforce multi-party Trust Criteria including safety rules, regulatory constraints, employment-law requirements, discriminatory-impact protections, and health-equity constraints.**

**Claim 212.** The method of Claim 207 wherein **no external system or ecosystem receives information sufficient to determine the underlying clinical rationale, behavioral indicator, or health-status condition that triggered the intervention.**

**Claim 213.** The method of Claim 207 wherein **interventions remain active and adaptive even when the individual is not actively engaged in medical care or clinical workflows.**

**Claim 214.** The method of Claim 207 wherein **intervention parameters are continuously recalibrated based on updated lifestyle-signal trajectories, behavioral-stability trends, or environmental-risk changes.**

## Family 11.3 — Cross-Domain Reuse & Zero-Marginal-Cost Intelligence

This family covers the PNX's distributed evidence-reuse layer, enabling lifestyle-signal outputs, risk indicators, and engagement events to be repeatedly reused—without new integrations or data exchanges—across clinical, financial, employer, research, and public-health systems. Zero-marginal-cost reuse transforms the entire evidence ecosystem.

**Licensing Value:** Applies to every analytics, clinical-decision-support, public-health, research, contracting, or patient-engagement platform; extremely high strategic IP leverage.

**Claim 215.** A system comprising, in any operable combination, one or more of:

**(a)** a **distributed evidence-reuse layer** configured to reuse lifestyle-signal outputs, behavioral-risk indicators, or privacy-bounded engagement events

across clinical care, benefit design, digital therapeutics, public-health analytics, patient-safety systems, and research workflows;

**(b)** a **zero-marginal-cost reuse engine** enabling repeated recomputation and redeployment of said outputs; and

**(c)** a **lineage layer** governing provenance, obligations, and permissible computational scope.

**Wherein** the system executes within a QPN-enabled infrastructure comprising at least one of: QPCs, Privacy Domains, Trust Criteria, PoT, Trust Blocks, or EasyAccess workflow threads.

**Claim 216.** The system of Claim 215 wherein **reuse occurs without creating new integrations, data-sharing agreements, or institutional connections, and wherein all cross-domain reuse relies exclusively on zero-knowledge outputs.**

**Claim 217.** The system of Claim 215 wherein **zero-marginal-cost reuse accelerates population-level trend detection, value-based contracting logic, medication-therapy-management processes, or longitudinal outcome-trajectory modeling.**

**Claim 218.** The system of Claim 215 wherein **evidence reuse enables cross-sector incentives spanning clinical, financial, workplace, community, or consumer-market environments without revealing underlying lifestyle, behavioral, or physiological signals.**

**Claim 219.** The system of Claim 215 wherein evidence **reuse enables environment-adaptive public-health interventions, including outbreak detection, epidemiologic-trend modeling, or community-risk mitigation, without exposing PHI or user-identifiable attributes.**

**Claim 220**. The system of Claim 215 wherein **all reused assets remain bound by immutable Trust Blocks documenting provenance, rights, obligations, regulatory lineage, sponsor permissions, and permissible computational scope enforced by the QPN.**

## GROUP 12 — PERSONAL HEALTH AGENTS, AUTONOMOUS WORKFLOW & CONTINUOUS OPTIMIZATION (Claims 221–240)

These claims cover agentic orchestration and privacy-preserving autonomy, including QPN-enabled autonomous coordination agents, continuous risk-model recalibration, longitudinal health-state modeling, and multi-party agentic workflow execution — all operating within QPCs.

## Family 12.1 — Personal Health Agents

This family covers personal health agents running inside the patient's PPN. These agents coordinate care, referrals, scheduling, follow-up, benefit optimization, condition-monitoring, and multi-party communication without exposing PHI to external applications or platforms. They execute cross-system actions using user-held rights and credentials ("dual-use rights"), combining clinical, behavioral, benefits, and environmental signals.

**Licensing Value:** High relevance for: Epic MyChart, Apple Health, Google Health, Amazon Clinic, Teladoc, One Medical, United / Optum, CVS / Aetna, and every digital health navigation app (Accolade, Castlight, Included Health). Also protects autonomous agentic AI inside clinical and consumer apps.

**Claim 221.** A system comprising, in any operable combination, one or more of:

**(a)** a **personal health agent** executing inside a patient's Personal Privacy Network (PPN);

**(b)** a **multi-source signal processor** configured to aggregate encrypted clinical, behavioral, lifestyle, environmental, and benefit-related indicators;

**(c)** an **action-orchestration engine** configured to initiate referrals, scheduling, follow-up tasks, or benefit-routing workflows using rights already possessed by the patient or clinician; and

**(d)** a **decision-support layer** configured to compute privacy-bounded eligibility, appropriateness, or risk signals to guide navigation actions;

**Wherein** the system executes within a QPN-enabled infrastructure comprising at least one of: Quantum Privacy Cells (QPCs); Privacy Domains; Trust Criteria; Proof-of-Trust (PoT); Trust Blocks; or EasyAccess workflow threads.

**Claim 222.** The system of Claim 221 wherein **personal health actions include selecting high-value providers, routing diagnostics, obtaining pricing, initiating prior authorization, or coordinating longitudinal care sequences.**

**Claim 223.** The system of Claim 221 wherein **the personal health agent interacts with external systems via zero-knowledge protocols that reveal only minimal eligibility, scheduling, or referral metadata.**

**Claim 224.** The system of Claim 221 wherein **the personal health agent automatically manages recurrent tasks including prescription renewals, monitoring reminders, diagnostic follow-ups, or goal tracking.**

**Claim 225.** The system of Claim 221 wherein **the personal health agent generates multi-party coordination threads among clinicians, caregivers, pharmacies, and payers without exposing PHI.**

**Claim 226.** The system of Claim 221 wherein **personal health intelligence is continuously recalibrated using federated lifestyle-signal trajectories.**

**Claim 227.** The system of Claim 221 wherein **clinician-facing interactions include triage support, contextual summaries, or safety alerts produced in zero-knowledge form.**

**Claim 228.** The system of Claim 221 wherein **personal health outputs are optimized for cost, convenience, safety, clinical appropriateness, benefit design, or patient preference.**

## Family 12.2 — Autonomous Multi-Party Workflow Threads & Agentic Task Execution

This family covers autonomous workflow engines that execute complex, multi-institution tasks (e.g., getting labs scheduled, coordinating pharmacy fulfillment, submitting benefit claims, routing forms, performing evidence checks) entirely within QPCs. These workflows operate as *agentic threads* that span multiple systems without exposing PHI or requiring integration.

**Licensing Value:** Covers all vendors building agentic care automation: Notable, Olive AI, Firefly, Ribbon Health, Xealth, Virta, Omada, prior-auth companies, claims automation engines, and care orchestration platforms.

**Claim 229.** A system comprising, in any operable combination, one or more of:

**(a)** an **autonomous workflow engine** configured to execute multi-step care, benefits, administrative, or safety workflows;

**(b)** an **inter-system thread manager** enabling multi-party coordination across EHRs, scheduling systems, pharmacy systems, payer portals, and public-health platforms;

**(c)** an **agentic task generator** configured to plan, decompose, and execute tasks using user-authorized rights; and

**(d)** a **privacy-bounded compliance layer** ensuring each step satisfies multi-party Trust Criteria and jurisdictional constraints;

**Wherein** the system executes within a QPN-enabled infrastructure comprising at least one of: QPCs; Privacy Domains; Trust Criteria; PoT; Trust Blocks; or EasyAccess workflow threads.

**Claim 230.** The system of Claim 229 wherein **the workflow engine performs cross-system actions including scheduling, claims submission, prior authorization, benefit routing, safety verification, or clinical workflow alignment.**

**Claim 231.** The system of Claim 229 wherein **agentic workflows include long-running, stateful processes coordinated across institutions without persistent identifiers or PHI exposure.**

**Claim 232.** The system of Claim 229 wherein **all workflow steps maintain immutable lineage encoded in Trust Blocks.**

**Claim 233.** The system of Claim 229 wherein **task decomposition is informed by federated patient-state models and lifestyle-signal trajectories.**

**Claim 234.** The system of Claim 229 wherein **the workflow engine automatically escalates tasks to clinicians, pharmacists, caregivers, or benefits teams when threshold criteria are met.**

**Claim 235.** The system of Claim 229 wherein **inter-system threads use zero-knowledge routing to prevent intermediaries from learning workflow intent or data context.**

## Family 12.3 — Dynamic AI Health-State Modeling, Continuous Risk Forecasting & Adaptive Plan Adjustment

These claims cover QPN-enabled continuous health-state modeling using federated, encrypted signals and adaptive plan updates (care plans, benefit plans, monitoring plans) without revealing underlying signals.

**Licensing Value:** Covers Mayo Clinic Platform, Kaiser AI initiatives, Epic BestCare, Google DeepMind health models, One Medical, Livongo/Omada metabolic engines, GLP-1 optimization platforms, risk engines (health plans, ACOs, reinsurers), and every chronic-care AI system.

**Claim 236.** A system comprising, in any operable combination, one or more of:

**(a)** a **federated health-state modeling engine**;

**(b)** a **multi-input ingestion layer** processing encrypted clinical, behavioral, social, environmental, and device signals;

**(c)** a **forecasting engine** computing privacy-bounded risk trajectories or condition-progression predictions; and

**(d)** an **adaptive plan-adjustment engine** configured to update care plans, benefit designs, monitoring protocols, or incentive structures;

**Wherein** the system executes within a QPN-enabled infrastructure comprising at least one of: QPCs; Privacy Domains; Trust Criteria; PoT; Trust Blocks; or EasyAccess workflow threads.

**Claim 237.** The system of Claim 236 wherein **health-state forecasts include deterioration risk, metabolic trajectory, adherence stability, relapse probability, hospitalization risk, or safety-threshold predictions.**

**Claim 238.** The system of Claim 236 wherein **adaptive plan adjustments include modifying interventions, altering benefit coverage, adjusting incentives, or initiating proactive outreach.**

**Claim 239.** The system of Claim 236 wherein **model training or recalibration occurs continuously, upon specified events, or on a specified schedule using zero-knowledge learning.**

**Claim 240.** The system of Claim 236 wherein **forecast outputs and plan updates are delivered without revealing underlying behavioral, lifestyle, or physiological signals.**

## GROUP 13 — PERSONAL HEALTH AGENTS, MULTI-PARTY COORDINATION & CONTINUOUS CARE NAVIGATION (Claims 241–260)

### Family 13.1 — Personal Health Agents for Care Navigation & Multi-Modal Support

**Claim 241.** A system comprising, in any operable combination, one or more of:

**(a)** a **Personal Health Agent** configured to interpret behavioral, contextual, environmental, care-related, or benefits-related signals;

**(b)** an **ingestion layer** receiving one or more encrypted or privacy-preserving inputs from devices, applications, services, or organizational systems;

**(c)** a **routing engine** computing care pathways, task sequences, referrals, or interventions; and

**(d)** a **coordination engine** managing cross-party scheduling, task completion, information requests, or follow-up actions without exposing sensitive information between parties.

**Wherein** the system executes within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 242.** The system of Claim 241 wherein the **Personal Health Agent triggers automated referrals, benefit lookups, navigation suggestions, or follow-up activities based on eligibility or appropriateness tests computed without revealing underlying user data.**

**Claim 243.** The system of Claim 241 wherein the **Personal Health Agent evaluates risk, social needs, stability indicators, or benefit constraints without exposing such data to external parties.**

**Claim 244.** The system of Claim 241 wherein **personal health pathways include one or more of: behavioral-health guidance, nutritional support, financial-wellness tools, social-care resources, or employer-provided benefits.**

### Family 13.2 — Dynamic Case-Management & Multi-Party Task Threads

**Claim 245.** **A method comprising**:

**(a)** detecting one or more case-management events or triggers;

**(b)** evaluating associated obligations, permissions, constraints, or requirements;

**(c)** initiating multi-party task threads involving one or more of: clinicians, caregivers, payers, employers, community organizations, or digital services; and

**(d)** executing coordination steps without disclosing underlying sensitive information to any participating entity.

**Wherein** the method executes within a QPN-enabled infrastructure comprising at least one of: QPCs, Privacy Domains, Trust Criteria, PoT, Trust Blocks, or EasyAccess workflow threads.

**Claim 246.** The method of Claim 245 wherein **case-management triggers include changes in stability, increased risk indicators, unmet social needs, benefit conflicts, or caregiver activity.**

**Claim 247.** The method of Claim 245 wherein **task threads persist across settings including in-person care, virtual care, workplace environments, home environments, retail environments, or transportation contexts.**

**Claim 248.** The method of Claim 245 wherein **each participating entity receives only the minimal privacy-bounded information necessary to complete its assigned task.**

### Family 13.3 — Prior Authorization, Eligibility, and Multi-Rail Determination

**Claim 249.** A system comprising, in any operable combination, one or more of:

**(a)** an **authorization engine** determining clinical, financial, or benefit-related appropriateness;

**(b)** an **eligibility-verification component** computing coverage or access determinations;

**(c)** a **benefit-logic component** applying rules related to pricing, tiers, limitations, or accumulators; and

**(d)** a **routing mechanism** transmitting approval, denial, redirection, or alternative-option outputs to relevant parties.

**Wherein** the system executes within a QPN-enabled infrastructure comprising at least one of: QPCs, Privacy Domains, Trust Criteria, PoT, Trust Blocks, or EasyAccess workflow threads.

**Claim 250.** The system of Claim 249 wherein **authorization outputs include approvals, alternative therapy recommendations, cost-optimized options, or network-tier routing.**

**Claim 251.** The system of Claim 249 wherein **no underlying clinical, behavioral, lifestyle, or risk-related information is revealed to any external system.**

**Claim 252.** The system of Claim 249 wherein **authorization outcomes may influence financial incentives, plan design recommendations, or care-pathway adjustments.**

## Family 13.4 — Follow-Up Automation, Adherence Monitoring & Early Intervention

**Claim 253.** **A method comprising**:

**(a)** monitoring one or more behavioral, physiological, contextual, or adherence-related signals;

**(b)** computing indicators of stability, deterioration, improvement, or relapse;

**(c)** generating automated follow-up actions or recommendations; and

**(d)** triggering context-appropriate interventions, referrals, or incentives.

**Wherein** the method executes within a QPN-enabled infrastructure comprising at least one of: QPCs, Privacy Domains, Trust Criteria, PoT, Trust Blocks, or EasyAccess workflow threads.

**Claim 254.** The method of Claim 253 wherein **follow-up actions include telehealth prompts, reminders, caregiver notifications, benefit updates, or micro-incentives.**

**Claim 255.** The method of Claim 253 wherein **relapse indicators are computed using anomaly detection, trajectory modeling, stress-load patterns, mobility changes, or environmental-risk factors.**

**Claim 256.** The method of Claim 253 wherein **no external entity can infer the underlying data used to generate follow-up determinations.**

## Family 13.5 — Multi-Sponsor Decision Coordination & Cross-Sector Routing

**Claim 257.** A system comprising, in any operable combination, one or more of:

**(a)** a **multi-sponsor coordination engine** allocating responsibilities, approvals, or incentives;

**(b)** a **routing layer** transmitting outputs to healthcare, employer, payer, community, or consumer ecosystems; and

**(c)** a **permissions framework** ensuring that participating entities receive only privacy-bounded signals.

**Wherein** the system executes within a QPN-enabled infrastructure comprising at least one of: QPCs, Privacy Domains, Trust Criteria, PoT, Trust Blocks, or EasyAccess workflow threads.

**Claim 258.** The system of Claim 257 wherein **coordination covers resource allocation, benefit sharing, incentive distribution, safety escalation, or therapeutic access.**

**Claim 259.** The system of Claim 257 wherein **permissions, obligations, and provenance attributes are enforced using immutable lineage constructs**.

**Claim 260.** The system of Claim 257 wherein **routing occurs without exposing identities, PHI, behavioral data, or risk-related information to any sponsor.**

## GROUP 14 — MULTI-SECTOR AGENTIC AUTOMATION & ZERO-KNOWLEDGE PROCESS EXECUTION (Claims 261–280)

### Family 14.1 — Zero-Knowledge Enterprise Workflow Automation

This family covers systems and methods enabling enterprises to automate internal processes (claims handling, HR workflows, financial approvals, customer support actions, compliance tasks, supply-chain events) using privacy-preserving computation.

Agents execute tasks without gaining access to private content, user data, or sensitive operational details.

**Licensing Value:** High relevance for: enterprise workflow platforms (ServiceNow, Workday, Salesforce), cloud providers (Microsoft, Amazon, Google), BPM vendors, HRTech platforms, RegTech systems.

**Claim 261.** A system comprising, in any operable combination, one or more of:

**(a)** a **workflow-automation engine** configured to evaluate encrypted or privacy-preserving inputs;

**(b)** a **rule-processing layer** determining task sequences, approvals, or escalations;

**(c)** a **multi-stakeholder coordination component** routing outputs to authorized enterprise systems; and

**(d)** an **execution layer** performing workflow actions without revealing underlying sensitive information.

**Wherein** the system executes within a QPN-enabled infrastructure comprising at least one of: QPCs, Privacy Domains, Trust Criteria, Proof-of-Trust, Trust Blocks, or EasyAccess workflow threads.

**Claim 262.** The system of Claim 261 wherein **outputs comprise workflow approvals, exception handling, task routing, compliance verification, or authorization results.**

**Claim 263.** The system of Claim 261 wherein **privacy-preserving inputs include encrypted documents, forms, signals, or structured records.**

**Claim 264.** The system of Claim 261 wherein no **enterprise system receives underlying PHI, financial details, personal identifiers, or behavioral data.**

**Claim 265.** The system of Claim 261 wherein **workflow steps are dynamically adjusted based on contextual, environmental, operational, or regulatory conditions.**

**Claim 266.** The system of Claim 261 wherein **enterprise actions are logged using immutable provenance constructs binding rights, obligations, and permissible computational scope.**

## Family 14.2 — Cross-Sector Business Process Agents

This family covers Personal Health Agents extended into enterprise domains to automate tasks that span healthcare, financial services, HR, benefits administration, consumer-online systems, and community services.

**Licensing Value:** Applies to: automation platforms (UiPath, Automation Anywhere), AI agent frameworks, HR/benefits engines, financial compliance systems, digital identity vendors.

**Claim 267.** **A method comprising**:

**(a)** receiving one or more encrypted signals related to a user event, benefit event, financial event, or operational event;

**(b)** determining task eligibility, priority, or routing criteria;

**(c)** activating a business-process agent to execute steps across enterprise systems; and

**(d)** producing privacy-bounded outputs consumable by downstream entities.

**Wherein** the method executes within a QPN-enabled infrastructure comprising at least one of: QPCs, Privacy Domains, Trust Criteria, PoT, Trust Blocks, or EasyAccess workflow threads.

**Claim 268.** The method of Claim 267 wherein **agent-executed workflows include benefit approvals, wellness program enrollment, financial routing, customer-support automation, or document verification.**

**Claim 269.** The method of Claim 267 wherein **cross-sector execution involves healthcare, financial, governmental, educational, or workplace systems.**

**Claim 270.** The method of Claim 267 wherein **each participating system receives only the minimal privacy-bounded output needed to complete its step.**

**Claim 271.** The method of Claim 267 wherein **no system learns the underlying event type or context.**

**Claim 272.** The method of Claim 267 wherein **business-process agents maintain immutable lineage binding decision criteria to permissible logic.**

## Family 14.3 — Zero-Knowledge Document & Form Processing

This family covers zero-knowledge extraction, validation, and approval of documents and forms, enabling enterprises to automate sensitive workflows (claims submission, eligibility verification, onboarding, underwriting) without exposing document content.

**Licensing Value:** Highly licensable to: DocuSign, Adobe, Notarize, enterprise onboarding platforms, claims processors, insurers, educational verification engines, fintech platforms.

**Claim 273.** A system comprising, in any operable combination, one or more of:

**(a)** a privacy-preserving document-ingestion module;

**(b)** a zero-knowledge extraction layer deriving structural fields without revealing raw content;

**(c)** a rule-evaluation module determining validity, completeness, or eligibility; and

**(d)** a routing module delivering decision outputs to authorized systems.

**Wherein** the system executes within a QPN-enabled infrastructure comprising at least one of: QPCs, Privacy Domains, Trust Criteria, PoT, Trust Blocks, or EasyAccess workflow threads.

**Claim 274.** The system of Claim 273 wherein **extracted outputs include zero-knowledge field existence checks, categorical tags, or binary eligibility markers.**

**Claim 275.** The system of Claim 273 wherein **documents include forms, claims, applications, identity records, certifications, or receipts.**

**Claim 276.** The system of Claim 273 wherein **no downstream system receives underlying document content.**

**Claim 277.** The system of Claim 273 wherein **incomplete or inconsistent submissions trigger automated follow-up requests.**

**Claim 278.** The system of Claim 273 wherein **document lineage is recorded using immutable trust metadata.**

**Claim 279.** The system of Claim 273 wherein **document data is never aggregated or centralized outside the user's Privacy Domain.**

**Claim 280.** The system of Claim 273 wherein **privacy-preserving document workflows support multi-party contracting, enrollment, triage, or verification.**

## GROUP 15 —PERSONAL HEALTH AGENTS FOR REAL-TIME GUIDANCE, COORDINATION & SUPPORT (Claims 281–290)

### Family 15.1 — Multi-Modal Personal Health Agents (PHAs) for Real-Time Guidance & Support

This family covers Personal Health Agents (PHAs) that interpret behavioral, contextual, environmental, physiological, and benefits-related signals to provide real-time guidance, tasking, navigation, scheduling, and continuous support across all touchpoints of a user's health journey.

PHAs operate as user-centered coordinators that unify interactions across clinical systems, benefits platforms, caregivers, digital therapeutics, devices, and consumer ecosystems — without exposing underlying data.

**Licensing Value**: High-value applicability for EHR vendors, digital navigation companies, telehealth systems, insurer care-management platforms, large consumer ecosystems, Apple/Google OS-level assistants, employer wellness solutions, and any vendor delivering AI-based personal health support.

**Claim 281.** A system comprising, in any operable combination, one or more of:

**(a)** a **Personal Health Agent** configured to interpret behavioral, contextual, environmental, care-related, physiological, or benefits-related signals;

**(b)** an **ingestion layer** receiving encrypted or privacy-preserving inputs from devices, applications, sensors, digital services, or organizational systems;

**(c)** a **decision engine** computing personalized tasks, navigation steps, referrals, or follow-up actions; and

**(d)** a **communication layer** delivering real-time guidance, requests, scheduling actions, or confirmations across user-authorized channels.

**Wherein** the system executes within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 282.** The system of Claim 281 wherein **the Personal Health Agent generates multi-modal outputs including text guidance, voice prompts, app-based notifications, task cards, reminders, or caregiver alerts.**

**Claim 283.** The system of Claim 281 wherein **the Personal Health Agent coordinates with clinical schedulers, referral systems, pharmacy systems, or care-management platforms without exposing underlying data.**

**Claim 284.** The system of Claim 281 wherein **tasks are sequenced based on urgency, safety requirements, user preferences, environmental context, or benefits eligibility.**

**Claim 285.** The system of Claim 281 wherein **the Personal Health Agent adapts outputs based on user stress levels, mobility state, symptoms, digital-engagement patterns, or physiological indicators.**

## Family 15.2 — Cross-Ecosystem Care Navigation & Unified Task Coordination

This family covers PHAs that coordinate tasks across clinical care, pharmacy workflows, benefits systems, financial-support pathways, caregiver networks, and community resources. Agents unify fragmented interactions into a single cross-ecosystem workflow without disclosing PHI between parties.

**Licensing Value**: Applies to telehealth integrations, health-system command centers, EHR workflow extensions, care-navigation vendors, PBM member-engagement systems, employer benefits platforms, and assistive-care coordination services.

**Claim 286.** **A method comprising:**

**(a)** receiving privacy-preserving task inputs from clinical, benefits, pharmacy, caregiver, or community entities;

**(b)** computing a unified task sequence aligned to safety, appropriateness, or user-defined preferences;

**(c)** routing task components to appropriate parties; and

**(d)** confirming task completion or requesting updated information without revealing sensitive underlying data.

**Wherein** the method executes within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 287.** The method of Claim 286 wherein **task routing spans clinical providers, pharmacies, labs, imaging centers, insurers, employers, caregivers, or digital-therapeutic systems.**

**Claim 288.** The method of Claim 286 wherein **the system resolves conflicts between competing tasks based on safety rules, regulatory requirements, or personalized constraints.**

**Claim 289.** The method of Claim 286 wherein **the Personal Health Agent automates data-gathering requests, benefit checks, or clinical-appropriateness queries in zero-knowledge form.**

**Claim 290.** The method of Claim 286 wherein **the system dynamically updates the task sequence based on new context, environmental changes, or user-provided responses.**

## GROUP 16 — MULTI-PARTY TRUST, SAFETY GOVERNANCE & CONTEXT-AWARE CONTROL LAYERS (Claims 291–300)

### Family 16.1 — Multi-Party Trust-Criteria Governance & Enforcement

This family covers systems that enforce multi-party Trust Criteria contributed by clinicians, caregivers, employers, safety authorities, regulators, and users. These criteria govern what actions PHAs, workflows, and applications may take, under what conditions, and with what oversight — all computed without revealing protected information.

**Licensing Value**: Applies to AI governance platforms, digital health systems, employer oversight engines, parental-control frameworks, safety-signal regulators, clinical decision-support vendors, and ecosystem trust-infrastructure providers.

**Claim 291.** A system comprising, in any operable combination, one or more of:

**(a)** a **governance layer** receiving Trust Criteria from multiple authorized contributors;

**(b)** a **constraint-evaluation engine** verifying whether proposed actions comply with safety, legal, clinical, contractual, or user-defined rules;

**(c)** an **override engine** enabling rule-bounded exception handling under restricted conditions; and

**(d)** an **action-authorization module** permitting or denying workflow steps without exposing underlying data.

**Wherein** the system executes within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 292.** The system of Claim 291 wherein **Trust Criteria are contributed by at least two of: clinicians, caregivers, employers, regulators, payers, or the user.**

**Claim 293.** The system of Claim 291 wherein **contributions include safety thresholds, environmental constraints, parental restrictions, employment-law protections, or clinical appropriateness rules.**

**Claim 294.** The system of Claim 291 wherein **the governance layer automatically resolves conflicting Trust Criteria based on predefined precedence logic.**

## Family 16.2 — Context-Aware Safety & Control for Multi-Modal Agents

This family covers context-aware safety layers that prevent Personal Health Agents from taking actions that are unsafe, unauthorized, or inappropriate given a user's state, environment, or risk trajectory — while retaining full privacy protections.

**Licensing Value:** Applicable to consumer AI assistants, clinical copilots, wearable-device platforms, robotics, autonomous-agent systems, employer safety tools, and digital-wellness ecosystems.

**Claim 295.** **A method comprising:**

**(a)** detecting real-time contextual indicators relevant to user safety, legality, appropriateness, or environmental risk;

**(b)** evaluating said indicators against multi-party Trust Criteria;

**(c)** determining whether an agent action, recommendation, or request is permitted; and

**(d)** preventing unauthorized or unsafe actions without exposing underlying context or signals.

**Wherein** the method executes within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 296.** The method of Claim 295 wherein **the system restricts actions during unsafe mobility states, harmful digital-content exposure, elevated stress levels, or clinically identified risk periods.**

**Claim 297.** The method of Claim 295 wherein **the system dynamically adjusts allowable agent behavior based on time, location, user condition, or environmental status.**

**Claim 298.** The method of Claim 295 wherein **control decisions are computed entirely within the user's Privacy Domain.**

**Claim 299.** The method of Claim 295 wherein **restricted actions include scheduling, referrals, purchase recommendations, medication-related workflows, or financial decisions.**

**Claim 300.** The method of Claim 295 wherein **control logic incorporates user-defined or caregiver-defined guardrails.**

## GROUP 17 — Autonomous Health Finance Optimization & Multi-Sponsor Settlement (Claims 301–320)

### Family 17.1 — Multi-Sponsor Settlement, Reconciliation & Value Apportioning Engines

This family protects systems that automatically allocate value, incentives, payments, rebates, subsidies, or settlement obligations across multiple sponsors—manufacturers, employers, payers, public-sector programs, community organizations, financial-assistance entities, or philanthropic contributors.

The finance engine computes settlement using privacy-bounded indicators, ensuring that no sponsor gains access to PHI, lifestyle signals, or personal financial details. This enables a universal multi-sponsor health-finance utility supporting personalized contracting, shared-savings models, incentive co-funding, price-support programs, and dynamic multi-party settlement.

**Licensing Value**: High-value coverage for: PBMs, payers, employers, fintech health-benefit platforms, drug-pricing engines, CMS programs, manufacturer rebate platforms, coupon networks, patient-assistance programs, and employer wellness finance systems.

**Claim 301.** A system comprising, in any operable combination, one or more of:

**(a)** a **multi-sponsor settlement engine** configured to allocate payment obligations, incentive amounts, subsidies, or rebate values across manufacturers, employers, payers, community organizations, or public programs;

**(b)** a **reconciliation module** configured to resolve cross-entity obligations using privacy-bounded transactional attributes;

**(c)** a **rules-evaluation layer** applying sponsor-specific constraints including contractual terms, eligibility rules, benefit-design logic, safety requirements, or regulatory obligations;

and,

**(d)** a **routing engine** configured to distribute settlement outputs without exposing underlying behavioral, clinical, or financial signals to any sponsor.

**Wherein** the system executes within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 302.** The system of Claim 301 wherein **settlement amounts are dynamically adjusted based on real-time eligibility indicators, adherence patterns, cost-sharing triggers, or public-program criteria.**

**Claim 303.** The system of Claim 301 wherein **sponsors receive only settlement outputs and never receive raw identifiers, personal financial details, behavioral indicators, or clinical data.**

**Claim 304.** The system of Claim 301 wherein **settlement is automatically recalculated when contextual factors change including time-of-day, location, environmental conditions, or benefit-design adjustments.**

**Claim 305.** The system of Claim 301 wherein **the reconciliation module maintains immutable lineage documenting sponsor contributions, permissible computational scope, and settlement-rule provenance.**

## Family 17.2 — Autonomous Health-Finance Orchestration & Precision Subsidy Allocation

This family covers automated orchestration of health-finance flows, including precision subsidy allocation, real-time affordability optimization, automatic application of financial assistance, and routing of value across multiple health-finance entities. The orchestration engine works without exposing PHI or personal financial vulnerability to any external party.

**Licensing Value:** Applicable to: payer affordability engines, manufacturer hub services, financial-assistance vendors, fintech health-wallet platforms, employer benefit-design platforms, public-program determination engines (e.g., Medicaid/CHIP/Medicare savings), and consumer-health marketplaces.

**Claim 306.** A **system comprising, in any operable combination, one or more of:**

**(a)** a **health-finance orchestration engine** configured to evaluate affordability rules, subsidy criteria, cost-sharing limits, or incentive eligibility;

**(b)** a dynamic**-allocation module** configured to direct subsidies, manufacturer support, employer credits, or public-program assistance to eligible transactions;

**(c)** a **privacy-bounded evaluation layer** configured to compute affordability indicators using encrypted inputs; and

**(d)** a **multi-channel routing component** configured to distribute financial assistance without revealing underlying health or behavioral information.

**Wherein the system executes within a QPN-enabled infrastructure comprising at least one of:** (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 307.** The system of Claim 306 wherein **subsidy allocation is conditioned on adherence trajectories, lifestyle-signal stability, safety thresholds, or environmental risk indicators computed in privacy-bounded form.**

**Claim 308.** The system of Claim 306 wherein **the orchestration engine automatically identifies the lowest-cost combination of sponsors capable of covering an event.**

**Claim 309.** The system of Claim 306 wherein **the routing component provides sponsors with anonymized settlement summaries that contain no PHI or financial-stress indicators.**

**Claim 310.** The system of Claim 306 wherein **multiple sponsors jointly fund a subsidy under a distributed co-financing model.**

## Family 17.3 — Distributed Financial-Integrity, Fraud Resistance & Lineage-Bound Settlement Proofs

This family protects distributed financial-integrity mechanisms used to detect fraud, prevent duplicate redemption, enforce lineage-bound eligibility, and validate multi-party financial flows without revealing sensitive personal information. These mechanisms enable compliant multi-entity financial coordination across the healthcare and non-healthcare economy.

**Licensing Value**: High defensive value for: payment processors, coupon networks, rebate clearinghouses, pharmacy systems, payers, manufacturers, financial-integrity platforms, and public-sector oversight engines.

**Claim 311.** A **system comprising, in any operable combination, one or more of:**

**(a)** a **financial-integrity engine** configured to detect duplicate transactions, anomalous routing patterns, or sponsor-inconsistent behaviors;

**(b)** a **fraud-resistant lineage-verification module** verifying the provenance of each settlement event;

**(c)** a **zero-knowledge validation layer** confirming compliance with sponsor-specific rules; and

**(d)** a **distributed event-ledger** capturing immutable settlement history.

**Wherein** the system executes within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 312.** The system of Claim 311 wherein **anomaly detection includes identifying suspicious time-density patterns, location inconsistencies, or sponsor-misaligned settlement sequences.**

**Claim 313.** The system of Claim 311 wherein **duplicate-redemption detection occurs using privacy-bounded transaction signatures that never expose identity data.**

**Claim 314.** The system of Claim 311 wherein **each settlement event is bound by immutable lineage identifying rights, obligations, constraints, and allowable computational scope.**

**Claim 315.** The system of Claim 311 wherein **only authorized participants can verify settlement validity without accessing underlying transactional details.**

## Family 17.4 — Autonomous Multi-Entity Clearing, Routing & Precision Cost Distribution

This family covers the autonomous clearing and precision distribution of financial obligations across manufacturers, payers, employers, health systems, public agencies, and community sponsors. The system calculates optimal routing paths using privacy-bounded signals, enabling multi-sponsor shared-savings models, precision program funding, and real-time multi-entity clearing.

**Licensing Value:** Covers: clearinghouses, PBMs, employer coalitions, public-sector health agencies, value-based-care payment engines, financial-infrastructure vendors, and multi-sponsor incentive networks.

**Claim 316.** A **system comprising, in any operable combination, one or more of:**

**a)** a **multi-entity clearing engine** configured to determine how financial obligations are apportioned across sponsors;

**(b)** a **routing engine** selecting optimal paths for distributing funds;

**(c)** a **constraint-evaluation module** ensuring compliance with sponsor-specific rules; and

**(d)** a **privacy-bounded output generator** providing settlement instructions without exposing personal signals.

**Wherein the system executes within a QPN-enabled infrastructure comprising at least one of:** (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 317.** The system of Claim 316 wherein **clearing decisions incorporate cost-effectiveness rules, productivity indicators, social-risk modifiers, or public-program equity constraints.**

**Claim 318.** The system of Claim 316 wherein **routing paths adapt dynamically to sponsor changes, environmental context, or population-level signals.**

**Claim 319.** The system of Claim 316 wherein **settlement outputs may trigger downstream incentives, plan adjustments, or corrective workflows.**

**Claim 320.** The system of Claim 316 wherein **no sponsor can determine the underlying clinical, behavioral, or lifestyle rationale for any financial allocation.**

## GROUP 18 — AI-Governed Continuous Safety, Fraud & Adversarial Resistance Systems (Claims 321–340)

### Family 18.1 — Continuous Adversarial-Resistance, Safety Monitoring & Threat-Adaptive Governance

This family protects real-time adversarial-resistance systems that continuously monitor for unsafe behaviors, adversarial manipulations, compromised workflows, model-tampering attempts, anomalous usage, or exploit patterns across clinical, financial, consumer, and cross-sector environments.

All detection and response logic executes inside Privacy Domains, ensuring that threat monitoring does not expose PHI, behavioral data, or cross-ecosystem identifiers.

**Licensing Value:** Covers hospital safety systems, payer fraud engines, PBMs, pharmacy networks, fintech fraud platforms, cybersecurity vendors, device OEMs, adversarial-AI defense platforms, model governance systems, and safety-monitoring engines used by major hyperscalers.

**Claim 321.** **A system comprising, in any operable combination, one or more of:**

**(a)** a **continuous threat-monitoring engine** configured to detect adversarial signals, anomalous patterns, unsafe usage trajectories, or cross-system manipulation attempts;

**(b)** a **safety-governance module** evaluating threat indicators under multi-party constraints including clinical rules, fraud-prevention requirements, regulatory obligations, or model-safety thresholds;

**(c)** a **zero-knowledge validation layer** confirming or rejecting suspicious events without revealing underlying data; and

**(d)** a **remediation engine** automatically triggering containment, throttling, pathway-rerouting, or sponsor-alert mechanisms.

**Wherein the system executes within a QPN-enabled infrastructure comprising at least one of:** (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 322.** The system of Claim 321 wherein **threat detection includes identification of abnormal timing densities, abnormal request signatures, multi-endpoint inconsistencies, or policy-violating access sequences.**

**Claim 323.** The system of Claim 321 wherein **adversarial-signal detection includes analysis of behavioral drift, AI-model stress indicators, out-of-distribution patterns, or adversarial-prompt structures.**

**Claim 324.** The system of Claim 321 wherein **containment measures include halting workflow execution, isolating compromised process branches, or escalating validation requirements.**

**Claim 325.** The system of Claim 321 wherein **only privacy-bounded threat-classification outputs are shared with external stakeholders.**

## Family 18.2 — Federated Fraud Detection, Multi-Entity Integrity Signals & Zero-Knowledge Validation

This family protects fraud detection and integrity validation frameworks that operate across payer, PBM, pharmacy, fintech, employer, and public-sector systems without sharing raw data.

Signals remain local to each stakeholder; only zero-knowledge confirmations or flags are exchanged.

**Licensing Value**: Strategic value for payers, PBMs, pharmacies, fintech reimbursement systems, reimbursement platforms, employer integrity modules, coupon networks, government benefit programs (SNAP/WIC/Medicaid), and cyber-fraud vendors.

**Claim 326.** **A system comprising, in any operable combination, one or more of:**

**(a)** a **federated fraud-signal engine** configured to ingest encrypted engagement, transaction, behavioral, or clinical-event signals;

**(b)** an **anomaly-detection layer** computing privacy-bounded integrity indicators;

**(c)** an **inter-entity validation framework** exchanging zero-knowledge proofs of fraud-relevant patterns; and

**(d)** a **routing module** propagating integrity alerts without revealing underlying signals.

**Wherein the system executes within a QPN-enabled infrastructure comprising at least one of:** (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 327.** The system of Claim 326 wherein **anomaly detection includes detection of duplicate redemptions, suspicious velocity patterns, inconsistent device signals, or multi-sponsor routing anomalies.**

**Claim 328.** The system of Claim 326 wherein **integrity validation occurs via zero-knowledge checks that disclose neither identity information nor contextual behavioral indicators.**

**Claim 329.** The system of Claim 326 wherein **cross-entity alerts include risk severity, affected transaction class, and required validation level without PHI disclosure.**

**Claim 330.** The system of Claim 326 wherein **validated fraud-flags trigger automated remediation workflows.**

## Family 18.3 — AI-Governed Clinical, Behavioral & Environmental Safety Enforcement

This family protects AI-governed systems enforcing clinical safety thresholds, environmental-risk constraints, and behavioral-stability requirements.

All evaluation occurs within the QPN, enabling zero-knowledge enforcement of guardrails for medication safety, mental-health signals, environmental exposures, digital-behavior risk, and clinician-supervised pathways.

**Licensing Value**: Relevant to: digital therapeutics, decision-support platforms, safety-monitoring tools, population-health vendors, medication-safety engines, pediatric protection tools, public-health platforms, GLP-1 optimization vendors, and employer risk-management systems.

**Claim 331.** **A system comprising, in any operable combination, one or more of:**

**(a)** a **safety-criteria evaluation engine** analyzing encrypted behavioral, clinical, environmental, or device-derived signals;

**(b)** a **rules-governance module** applying multi-party safety thresholds;

**(c)** a **recommendation layer** generating privacy-bounded approvals, denials, suppressions, or risk-adaptive adjustments; and

**(d)** an **enforcement mechanism** executing safety-based workflow modifications.

**Wherein** the system executes within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 332.** The system of Claim 331 wherein **behavioral-safety evaluation includes detection of depressive-risk patterns, stress-trajectory instability, self-harm risk signals, escalating compulsive activity, or executive-function instability.**

**Claim 333.** The system of Claim 331 wherein **environmental-safety evaluation includes exposure to harmful allergens, pollutants, temperature extremes, neighborhood risk, food-environment risk, or transportation hazards.**

**Claim 334.** The system of Claim 331 wherein **clinical-safety evaluation includes medication-interaction detection, adherence destabilization, worsening vital-signal trajectories, or contraindication evaluation.**

**Claim 335.** The system of Claim 331 wherein **safety enforcement includes suppressing harmful digital content, adjusting therapeutic pathways, notifying authorized clinicians, or activating emergency workflows.**

## Family 18.4 — Adversarial-Robust AI Reasoning, Model-Lineage Validation & Autonomous Red-Teaming

This family protects adversarial-resistance for AI reasoning systems, including lineage-bound validation, zero-knowledge model-safety checks, and continuous autonomous red-teaming.

The system ensures AI-generated outputs are safe, lawful, and aligned with Trust Criteria without exposing training data or user context.

**Licensing Value**: Critical IP for model providers (OpenAI, Google Gemini, Anthropic, Meta, Microsoft, Apple), hospitals, payers, AI-safety vendors, agentic-reasoning platforms, and any regulated AI application.

**Claim 336.** **A system comprising, in any operable combination, one or more of:**

**(a)** an **adversarial-robust reasoning engine** performing safety-bounded analysis;

**(b)** a **model-lineage validator** verifying provenance of model components, fine-tunings, or safety overlays;

**(c)** a **privacy-bounded red-teaming module** evaluating model behavior under synthetic adversarial scenarios; and

**(d)** a **zero-knowledge verification layer** ensuring model outputs comply with safety constraints.

**Wherein the system executes within a QPN-enabled infrastructure comprising at least one of:** (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 337.** The system of Claim 336 wherein **autonomous red-teaming tests include prompt-injection detection, jailbreak detection, hallucination-risk profiling, or chain-of-thought stability testing.**

**Claim 338.** The system of Claim 336 wherein **model-lineage validation includes confirming regulatory compliance, sector-specific safety overlays, or institution-defined value constraints.**

**Claim 339.** The system of Claim 336 wherein **zero-knowledge model-output verification discloses only pass/fail status or approved categories without revealing reasoning content or sensitive prompts.**

**Claim 340.** The system of Claim 336 wherein **adversarial-resistance actions include suppressing unsafe output, escalating to human review, or modifying reasoning pathways.**

## GROUP 19 — Population-Scale Predictive Models & Early-Warning Grids (Claims 341–360)

### Family 19.1 — Population-Scale Predictive Models & Federated Forecasting Engines

This family protects systems that compute population-level forecasts—clinical, behavioral, environmental, epidemiologic, or utilization-related—using federated, privacy-bounded signals derived from distributed QPCs. These predictions never require centralizing raw PHI, lifestyle signals, device telemetry, or environmental exposures. Only aggregated, zero-knowledge outputs flow upward into national or multi-institutional forecasting layers.

**Licensing Value**: High-value coverage for public-health agencies, payers, biopharma, epidemiology platforms, AI-forecast vendors, hospital command centers, mobility/transportation forecasters, CMS/CDC contractors, hyperscalers developing population-modeling engines, and state-level health-information networks.

**Claim 341.** **A system comprising, in any operable combination, one or more of:**

**(a)** a **distributed forecasting engine** configured to ingest encrypted, privacy-bounded signals from individual or institutional endpoints;

**(b)** a **population-model construction layer** computing aggregated predictions of risk trajectories, utilization patterns, demand curves, or emergent phenomena;

**(c)** a **zero-knowledge aggregation module** ensuring that only non-identifying statistical outputs are exposed; and

**(d)** a **dissemination framework** providing authorized stakeholders with prediction summaries, alerts, resource-allocation guidance, or anonymous personalized notifications to patients and their clinicians.

**Wherein the system executes within a QPN-enabled infrastructure comprising at least one of:** (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 342.** The system of Claim 341 wherein **forecasting includes prediction of clinical deterioration, hospitalization demand, medication-adherence destabilization, or chronic-disease progression.**

**Claim 343.** The system of Claim 341 wherein **forecasting includes prediction of behavioral-risk drift, stress-trajectory instability, mobility-pattern shifts, or nutrition-linked volatility.**

**Claim 344.** The system of Claim 341 wherein **forecasting includes prediction of sector-level impacts including workforce availability, school-system strain, transportation disruption, or community-resource utilization.**

**Claim 345.** The system of Claim 341 wherein **only privacy-bounded aggregated statistics are transmitted to health plans, employers, agencies, or manufacturers.**

**Claim 346.** The system of Claim 341 wherein **forecasts dynamically update in response to changing encrypted signals from QPCs.**

**Claim 347.** The system of Claim 341 wherein **prediction confidence scores incorporate institutional Trust Criteria or jurisdiction-specific regulatory constraints.**

## Family 19.2 — Early-Warning Grids & Distributed Signal Detection Systems

This family protects early-warning systems that identify emerging anomalies—clinical, behavioral, environmental, epidemiologic, or pharmacovigilance-related—using federated, privacy-bounded signal integration.

This includes outbreak detection, medication-safety detection, adverse-event clustering, social-risk escalation, and environmental-risk patterning.

**Licensing Value**: Relevant to population-health surveillance, CDC/state surveillance grids, WHO-scale systems, payer fraud/safety analytics, pharmacovigilance vendors, hospital safety systems, remote-patient-monitoring vendors, mental-health risk platforms, and workforce-readiness forecasters.

**Claim 348.** **A system comprising, in any operable combination, one or more of:**

**(a)** a **distributed signal-detection engine** analyzing encrypted event patterns across heterogeneous endpoints;

**(b)** an **anomaly-detection module** identifying statistically significant deviations from baseline;

**(c)** a **zero-knowledge alert-generation** component creating privacy-bounded early-warning outputs; and

**(d)** a **routing engine delivering alerts** to authorized stakeholders without exposing user-level data.

**Wherein the system executes within a QPN-enabled infrastructure comprising at least one of:** (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 349.** The system of Claim 348 wherein **anomalies include spikes in symptoms, adverse-event clusters, environmental exposures, behavioral-risk surges, or device telemetry instability.**

**Claim 350.** The system of Claim 348 wherein **early-warning alerts include severity level, time-window density, geographic relevance, or recommended response tier.**

**Claim 351.** The system of Claim 348 wherein **anomaly detection incorporates multi-party safety thresholds contributed by clinicians, public-health agencies, employers, or caregivers.**

**Claim 352.** The system of Claim 348 wherein **early-warning outputs exclude identifiers, timestamps, or patterns that could re-identify users.**

**Claim 353.** The system of Claim 348 wherein **detection occurs continuously, triggered by encrypted incremental updates from QPCs.**

## Family 19.3 — Digital Epidemiology, Outbreak Analytics & Public-Health Intelligence

This family protects digital-epidemiology mechanisms enabling real-time outbreak detection, transmission-path inference, environmental-risk modeling, and cross-population intelligence—without sharing raw PHI, mobility data, or behavioral signals.

All epidemiologic inference is performed inside Privacy Domains using privacy-bounded mathematics.

**Licensing Value:** Applies to CDC/WHO contractors, state health departments, mobility-signal analytics companies, wastewater-signal platforms, epidemiology AI vendors, transport systems, hospital networks, workplace health/safety systems, and environmental-risk monitoring vendors.

**Claim 354.** **A system comprising, in any operable combination, one or more of:**

**(a)** an **epidemiologic-inference engine** computing privacy-bounded estimates of disease prevalence, transmission paths, or environmental-exposure patterns;

**(b)** a **distributed signal-fusion module** combining encrypted lifestyle, mobility, environmental, or clinical-event indicators;

**(c)** a **zero-knowledge prevalence-estimation layer** producing non-identifying epidemiologic statistics; and

**(d)** a **dissemination engine** routing outputs to authorized public-health entities or stakeholders.

**Wherein the system executes within a QPN-enabled infrastructure comprising at least one of:** (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

**Claim 355.** The system of Claim 354 wherein **epidemiologic inference includes computation of reproductive number estimates, outbreak acceleration, exposure density, or environmental-risk amplification.**

**Claim 356.** The system of Claim 354 wherein **transmission-path inference includes zero-knowledge linkage of correlated signals without identifying individuals.**

**Claim 357.** The system of Claim 354 wherein **environmental-exposure modeling includes air-quality signals, pollutant spikes, temperature extremes, or allergen patterning.**

**Claim 358.** The system of Claim 354 wherein **epidemiologic alerts incorporate confidence intervals, geographic granularity, or recommended mitigation pathways.**

**Claim 359.** The system of Claim 354 wherein **only privacy-bounded aggregated statistics are shared with public-health agencies.**

**Claim 360.** The system of Claim 354 wherein the **epidemiologic model dynamically recalibrates based on evolving encrypted inputs, new Trust Criteria, or updated environmental conditions.**

## GROUP 20 — ANONYMOUS PATIENT SAFETY & PUBLIC-HEALTH SYSTEMS (CLAIMS 361–384)

### Family 20.1 — Anonymous Real-Time Patient Safety & Public-Health Interaction Systems

This family covers systems enabling **anonymous, privacy-preserving real-time interaction** between patients, safety engines, clinicians, digital therapeutics, and public-health entities. All interactions occur without revealing patient identity unless the patient explicitly authorizes it.

These capabilities support early-warning grids, safety interventions, symptom clarification, anomaly validation, and remote support without PHI disclosure.

**Licensing Value:** High value for state/CDC surveillance, remote-monitoring platforms, digital therapeutics, telehealth safety layers, mental-health crisis systems, care-navigation systems, and AI-driven early warning vendors.

**Claim 361.** A system comprising, in any operable combination, one or more of:

**(a)** an **anonymous interaction engine** configured to initiate real-time communication with a patient or authorized participant without disclosing the identity of the patient to any other participant;

**(b)** a **signal-refinement subsystem** that receives encrypted or privacy-preserved telemetry, symptom reports, behavioral signals, device readings, or caregiver feedback and processes them to improve the precision of safety assessments;

**(c)** a **population-level analytics layer** that detects encrypted or privacy-preserved early-warning patterns including metabolic deterioration, medication-safety anomalies, behavioral-health instability, infectious-disease emergence, environmental exposures, or post-discharge fragility;

**(d)** an **intervention-routing component** that delivers safety alerts, decision support, or recommended actions to one or more authorized participants—including clinicians, caregivers, digital therapeutics, connected devices, or community organizations—without exposing the identity of any underlying patient;

**(e)** a **privacy-preserved communication interface** through which anonymous symptom-checks, clarifying questions, device pings, or care-coordination requests are transmitted and received; and

**(f)** a **safety-response orchestration engine** that triggers downstream clinical, behavioral, or public-health workflows upon detection of risk conditions.

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads, and wherein patient identity, PHI, or identifiable context remains cryptographically hidden from all participants unless explicit authorization is granted by the patient.

**Claim 362.** The system of Claim 361, wherein **the anonymous interaction engine delivers personalized decision support to a patient without exposing any underlying PHI to clinicians, payers, vendors, or public-health authorities.**

**Claim 363.** The system of Claim 361, wherein **caregiver or clinician interaction occurs through privacy-preserved proxy identifiers that cannot be correlated to the identity of the patient without patient authorization.**

**Claim 364.** The system of Claim 361, wherein **public-health agencies receive only population-level or zero-knowledge outputs and cannot access patient-identifiable information absent lawful emergency-unmasking criteria expressly authorized by the patient.**

**Claim 365.** The system of Claim 361, wherein **anonymous interactions include one or more of: symptom-checks, medication prompts, mental-health screening questions, safety-threshold validations, anomaly confirmations, device telemetry requests, or outreach to designated caregivers.**

**Claim 366.** The system of Claim 361, wherein **the intervention-routing component initiates real-time interactions with external systems—including digital therapeutics, remote-monitoring devices, behavioral-health platforms, or telehealth infrastructure—while preserving patient anonymity.**

## Family 20.2 — Legal & Cryptographic Privacy Protection of Patient-Controlled Data

This family covers mechanisms ensuring that patient-controlled information in PPNs remains **constitutionally and cryptographically irrecoverable** unless the patient voluntarily authorizes disclosure. Clinicians may view the information ephemerally through QPC-bounded access, but they never acquire possession, enabling strong Fifth-Amendment protections.

**Licensing Value:** High relevance for EHR vendors, mental-health systems, reproductive-health platforms, safety-critical clinical apps, legal-privacy systems, digital therapeutics, and any system requiring strong constitutional privacy posture.

**Claim 367.** **A system comprising, in any operable combination, one or more of:**

**(a)** a **patient-controlled data-custody mechanism** that maintains personal information exclusively within a patient-controlled domain;

**(b)** a **cryptographic irreversibility engine** that prevents decryption or release of patient information absent an affirmative authorization action performed by the patient;

**(c)** a **clinician-access subsystem** enabling ephemeral review of patient-controlled information without transferring custody, possession, or long-term retention to the clinician or provider organization;

**(d)** a **contractual-binding mechanism** by which a clinician's QPC or Privacy Domain agrees to honor patient-imposed constraints on redisclosure, retention, or permissible use of patient-controlled information;

**(e)** a **provider-records subsystem** configured to store only provider-generated notes, diagnoses, or treatment decisions required by legal retention rules while excluding patient-controlled underlying PHI; and

**(f)** a **disclosure-governance module** enforcing that identifiable patient information may be disclosed only through explicit patient authorization.

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v)

Trust Blocks; or (vi) EasyAccess workflow threads, and wherein any attempt to compel patient authorization constitutes a prohibited testimonial act under applicable constitutional protections, rendering patient-controlled information legally and technically irrecoverable absent patient consent.

**Claim 368.** The system of Claim 367, wherein **clinician non-possession is enforced by prohibiting export, caching, local storage, screenshotting, or re-encoding of patient-controlled information within any clinician or provider system.**

**Claim 369.** The system of Claim 367, wherein **the provider-records subsystem stores only a clinical note, provider reasoning, orders, and necessary documentation while excluding raw signals or content supplied exclusively through the patient's PPN.**

**Claim 370.** The system of Claim 367, wherein **the contractual-binding mechanism is executed automatically upon clinician access and is immutably recorded in a Trust Block.**

**Claim 371.** The system of Claim 367, wherein **the disclosure-governance module prevents any provider, clinician, or business associate from releasing identifiable information in response to subpoenas, warrants, public-health orders, or administrative demands unless the patient invokes affirmative authorization.**

## Family 20.3 — Nationwide Privacy-Preserving Safety, Public-Health & Research Grid

This family covers a nationwide grid combining patient-safety monitoring, post-market surveillance, population-level epidemiology, and continuous real-world research, all executed inside QPC-bounded cleanrooms. The system interacts anonymously with individuals and clinicians while providing large-scale intelligence without PHI leakage.

**Licensing Value:** Major applicability for NIH, CDC, FDA, state health departments, pharma safety systems, CROs, decentralized-trial vendors, academic research networks, and real-world data/analytics platforms.

**Claim 372.** **A system comprising, in any operable combination, one or more of:**

**(a)** a **distributed national safety-analytics layer** executing population-level safety, risk, and epidemiologic computations over encrypted or privacy-preserved inputs from millions of participants;

**(b)** a **real-time post-market surveillance subsystem** detecting safety signals relating to drugs, biologics, devices, diagnostics, digital therapeutics, or AI-driven tools without centralizing identifiable PHI;

**(c)** a **continuous observational-research platform** performing eligibility checks, consent workflows, outcome tracking, adverse-event detection, and trial-protocol tasks inside QPC-bounded Privacy Domains;

**(d)** a **dual-use integration architecture** enabling health-preserving computation using external ecosystems—including consumer apps, e-commerce platforms, financial-services rails, transportation networks, or digital-media systems—without releasing PHI to such systems;

**(e)** a **CRAACO-enabling research-integration engine** embedding trial participation into routine clinical and behavioral workflows; and

**(f)** a **verification, attribution, and value-pooling mechanism** configured to quantify and redistribute savings or value created across care delivery, public health, patient safety, and research activities.

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads, and wherein all analytics are performed without centralizing identifiable PHI and without revealing any individual's identity to public-health agencies, researchers, manufacturers, or other participants unless expressly authorized by the patient.

**Claim 373.** The system of Claim 372, wherein **the observational-research platform supports real-time Phase 4 studies, confirmatory trials, pragmatic trials, adaptive registries, or post-market evaluations**.

**Claim 374.** The system of Claim 372, wherein **dual-use infrastructure enables zero-marginal-cost reuse of computation, data, or engagement signals across clinical, financial, consumer, and public-health sectors**.

**Claim 375.** The system of Claim 372, wherein **research participation is triggered by privacy-preserved matching algorithms executed inside QPCs based on encrypted behavioral, clinical, environmental, or engagement indicators.**

**Claim 376**. The system of Claim 372, wherein **the safety-analytics layer supports anonymous real-time interaction with patients to obtain clarifying signals or trigger interventions while preserving patient anonymity.**

## Family 20.4 — Anonymous Safety Interaction & Provider-Side Early-Warning Systems

This family covers systems that enable **clinicians and care teams to receive real-time, privacy-preserved safety signals**, interact anonymously with patients, and coordinate early-warning responses **without PHI disclosure**, unless expressly authorized.

**Applies to:** hospitals, digital-therapeutic vendors, care-management platforms, remote-monitoring vendors, mental-health systems, population-health units, ACOs, multi-specialty groups, and telehealth platforms.

**Claim 377.** **A system comprising, in any operable combination, one or more of:**

**(a)** a **clinician-side anonymous-interaction module** configured to receive privacy-preserved early-warning signals, summary risk indicators, or zero-knowledge alerts without revealing patient identity;

**(b)** a **clinician-engagement engine** enabling clinicians to send clarifying questions, device-telemetry requests, care-plan adjustments, or follow-up prompts to an anonymous patient via privacy-preserved channels;

**(c)** a **care-team routing subsystem** that assigns anonymous safety tasks, escalations, or workload notifications to authorized clinicians, pharmacists, behavioral-health specialists, or care coordinators without exposing patient-identifiable information;

**(d)** a **bidirectional verification engine** that validates patient-submitted signals, symptom reports, or device readings using encrypted or privacy-preserved computation;

**(e)** an **intervention-safety module** that triggers clinician-side tasks—such as medication review, outreach, telehealth scheduling, or crisis-response activation—based on privacy-preserved risk patterns; and

**(f)** a **provider-infrastructure interface** enabling hospitals or clinics to incorporate anonymous safety signals within existing workflows without storing or handling identifiable PHI.

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads, and wherein no clinician or provider system gains access to identifiable PHI unless the patient explicitly authorizes disclosure.

**Claim 378.** The system of Claim 377, wherein **clinician interactions are mapped to privacy-preserved proxy identifiers that preserve continuity of care without revealing patient identity.**

**Claim 379.** The system of Claim 377, wherein **the clinician-engagement engine supports asynchronous or synchronous communication—including secure messaging, telehealth prompts, crisis-line escalation, or automated outreach—without revealing patient identity.**

**Claim 380.** The system of Claim 377, wherein **the provider-infrastructure interface ensures provider systems receive only de-identified or zero-knowledge outputs, preventing clinicians or IT systems from reconstructing patient-identifiable information.**

**Claim 381.** The system of Claim 377, wherein **the care-team routing subsystem automatically allocates clinical tasks based on clinician role, capacity, licensure, specialty, or proximity, while preserving patient anonymity.**

**Claim 382.** The system of Claim 377, wherein the **clinician-side module integrates with existing EMRs, EHRs, clinical dashboards, or telehealth systems through privacy-preserved EasyAccess workflow threads without requiring data ingestion.**

**Claim 383.** The system of Claim 377, wherein **clinician tasks triggered by early-warning signals must be annotated using privacy-preserved note-creation that prevents incorporation of identifiable PHI into institutional systems unless authorized by the patient.**

**Claim 384.** The system of Claim 377, wherein **the system supports reciprocal anonymous interaction between clinicians and caregivers, enabling multi-party coordination without revealing patient identity to any participant.**

## GROUP 21 — PARALLEL PUBLIC-HEALTH & RESEARCH SYSTEMS (CLAIMS 385-392)

### Family 21.1 — Privacy-Preserving Public-Health Decision Support & Population-Level Alerts

This family protects the systems that enable public-health agencies to receive early-warning indicators, outbreak signals, environmental patterns, and chronic-disease deterioration signals **without identifiable PHI**.

**Licensing value:** CDC, state health departments, global health organizations, wastewater-signal vendors, environmental-risk companies, syndromic-surveillance systems.

**Claim 385.** **A system comprising, in any operable combination, one or more of:**

**(a)** a **population-scale early-warning layer** that computes privacy-preserved outbreak signals, chronic-disease deterioration markers, substance-use risk patterns, environmental exposures, or safety anomalies;

**(b)** a **public-health routing module** delivering non-identifiable alerts, geographic gradients, or population-level risk information to authorized public-health entities;

**(c)** a **zero-knowledge public-health query engine** enabling agencies to request aggregated or privacy-bounded statistics without accessing identifiable PHI;

**(d)** a **syndromic-pattern inference engine** detecting clusters or trajectories based on privacy-preserved data from QPC-bounded clinical, behavioral, environmental, or device-generated sources;

**(e)** a **lawful-unmasking gateway** that allows patient identity to be revealed only when emergency thresholds are met **and** when the patient explicitly authorizes disclosure; and

**(f)** a **public-health integration subsystem** enabling cross-agency coordination using de-identified patterns, trends, or risk gradients.

**Wherein** the system executes within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads, and wherein public-health entities never receive patient-identifiable information unless the patient explicitly authorizes unmasking.

**Claim 386.** The system of Claim 385, wherein **the zero-knowledge public-health query engine provides privacy-preserved statistics including prevalence, incidence, risk-trajectory slopes, cluster dispersion, or comparative baselines.**

**Claim 387.** The system of Claim 385, wherein **emergency unmasking requires patient consent verified via Trust Criteria inherited from upstream Trust Blocks.**

**Claim 388.** The system of Claim 385, wherein **outbreak alerts are triggered by deviations detected using privacy-preserved anomaly-detection models across clinical, behavioral, environmental, or mobility-signal categories.**

## Family 21.2 —Privacy-Preserving Real-World Evidence & Continuous Observational Research

This family extends the research-layer claims with additional rights covering RWE generation, protocol automation, eligibility matching, and trial-execution inside QPC cleanrooms.

**Licensing value:** pharma, NIH, FDA, CROs, DCT vendors, academic medical centers, RWE vendors.

**Claim 389.** **A system comprising, in any operable combination, one or more of:**

**(a)** a **real-world-evidence computation layer** performing safety, effectiveness, adherence, quality-of-life, and cost-effectiveness analytics over privacy-preserved inputs;

**(b)** a **protocol-automation engine** executing study procedures—including eligibility checks, randomization, consent, outcome tracking, adverse-event logging, or statistical monitoring—inside QPC-bounded domains;

**(c)** a **privacy-preserved eligibility-matching engine** using encrypted clinical, behavioral, genomic, environmental, or engagement indicators;

**(d)** a **decentralized research-coordination subsystem** enabling multi-site collaboration without centralizing PHI;

**(e)** a **longitudinal synthetic-cohort engine** generating privacy-preserved cohort signals, control-arm estimates, or comparator trajectories; and

**(f)** a **cross-sector research-reuse mechanism** enabling data and computation used for clinical care to be reused for observational research at zero marginal cost.

**Wherein** the system executes within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads, and wherein identifiable PHI is never centralized or revealed unless expressly authorized by the patient.

**Claim 390.** The system of Claim 389, wherein **trial monitoring, statistical quality checks, and adaptive stopping rules are executed entirely within Privacy Domains, preventing access to identifiable PHI by sponsors, CROs, or regulators.**

**Claim 391.** The system of Claim 389, wherein **eligibility-matching uses encrypted similarity metrics, privacy-preserved phenotype embeddings, or federated vector representations.**

**Claim 392.** The system of Claim 389, wherein **observational research is embedded into routine clinical workflows and executed without requiring new integrations, data extraction, or EHR modification.**

## GROUP 22 — AUTONOMOUS MULTI-AGENT ECONOMIC ORCHESTRATION (CLAIMS 393-416)

### Family 22.1 — Autonomous Multi-Agent Negotiation, Resource Allocation & Value Optimization

This family protects foundational mechanisms for autonomous multi-agent economic coordination, including negotiation engines, incentive-balancing frameworks, resource-allocation markets, and ecosystem-wide optimization executed entirely within QPC-bounded environments.

These claims establish the core architecture for agentic commerce across clinical, financial, workplace, consumer, supply-chain, and public-sector systems.

**Licensing Value:** Protects the AI-economy orchestration layer required by hyperscalers, fintech ecosystems, employer platforms, payers, manufacturers, supply-chain networks, logistics platforms, SaaS vendors, and autonomous-agent frameworks. Extremely high strategic value as global AI-agent economies emerge.

**Claim 393.** A system comprising, in any operable combination, one or more of:

**(a)** one or more **autonomous negotiation engines** configured to compute bargaining positions, trade-offs, exchange options, or incentive-compatible strategies across multiple stakeholders using privacy-preserved inputs;

**(b)** a **resource-allocation layer** computing optimal or near-optimal distribution of tasks, incentives, payments, attention, computation, or physical resources using encrypted or privacy-bounded indicators;

**(c)** a **multi-agent coordination engine** managing proposal exchange, counter-proposal generation, prioritization, and outcome selection without revealing underlying user-specific or stakeholder-specific data;

**(d)** a **tokenized-value flow engine** applying contribution-weighted rules, Trust-Criteria constraints, contractual lineage, and ecosystem governance requirements to dynamic value-sharing determinations; and

**(e)** a **cross-ecosystem routing subsystem** delivering privacy-bounded economic signals to authorized participants across healthcare, employer, financial, consumer, supply-chain, or governmental systems.

**Wherein** the system executes within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads,

**and wherein** no participant receives raw identifiers, PHI, behavioral context, or sensitive economic indicators of other participants.

**Claim 394.** The system of Claim 393 wherein **the autonomous negotiation engine evaluates fairness, risk, preference, or safety constraints contributed by clinicians, caregivers, employers, regulators, or the user.**

**Claim 395.** The system of Claim 393 wherein **multi-agent negotiation includes dynamic market-clearing, auction-based selection, matching, or federated bargaining executed without revealing underlying preferences, costs, or constraints.**

**Claim 396.** The system of Claim 393 wherein **the resource-allocation layer incorporates cryptographically protected clinical, environmental, behavioral, logistical, supply-chain, or financial indicators to compute optimal distribution of resources.**

**Claim 397.** The system of Claim 393 wherein **the cross-ecosystem routing subsystem delivers economic-alignment outputs to one or more of: employers, payers, manufacturers, community organizations, marketplaces, telehealth systems, logistics systems, transportation networks, or consumer-online platforms.**

**Claim 398.** The system of Claim 393 wherein **negotiation outputs include at least one of: incentive-alignment weights, settlement recommendations, optimal-path proposals, value-distribution options, or conflict-resolution selections.**

**Claim 399.** The system of Claim 393 wherein **all negotiation and allocation computations are logged as immutable Trust Blocks documenting obligations, rights, provenance, and permissible computational scope.**

**Claim 400.** The system of Claim 393 wherein **multi-agent negotiation occurs continuously and adapts dynamically to new cryptographically protected signals including changes in supply, demand, risk, preferences, or environmental context.**

**Claim 401.** The system of Claim 393 wherein **the tokenized-value flow engine automatically redistributes value across stakeholders based on contribution, risk, benefit, or alignment with ecosystem-governance rules.**

**Claim 402.** The system of Claim 393 wherein **no participant, including negotiating agents, can infer the identity, attributes, or economic position of any other stakeholder.**

## Family 22.2 — Agentic Marketplace Optimization & Cross-Agent Contracting

This family covers the foundational infrastructure enabling autonomous agents to negotiate, contract, bid, select partners, coordinate work, and optimize multi-party economic activity. All interactions occur within QPC-bounded Privacy Domains, ensuring that underlying clinical, behavioral, economic, or contextual data remain private.

These capabilities are essential for emerging agent economies where autonomous agents operate across healthcare, logistics, financial services, enterprise ecosystems, consumer services, and public-sector domains.

**Licensing Value:** Protects core infrastructure for autonomous marketplace behavior — agent–agent contracting, negotiation, routing of work, dynamic bundling of services, price/path optimization, risk-aware selection, and automatic enforcement of QPC-bounded constraints.

High value for hyperscalers, enterprise SaaS networks, AI agent frameworks, fintech rails, health marketplaces, logistics engines, and consumer ecosystems.

**Claim 403.** A system comprising, in any operable combination, one or more of:

**(a)** an **agentic contracting engine** configured to negotiate, generate, validate, or execute agreements between autonomous agents using privacy-preserved inputs;

**(b)** a **marketplace-optimization layer** computing cost, value, safety, or preference-aligned selection among competing agents or resource providers;

**(c)** a **federated offer–response subsystem** managing proposal generation, bid evaluation, counter-offers, and settlement outcomes without revealing underlying stakeholder data;

**(d)** a **risk-modulated routing engine** directing tasks, contracts, or economic flows to optimal agent clusters based on encrypted contextual indicators; and

**(e)** a **compliance-verification module** applying Trust Criteria, safety constraints, contractual obligations, or jurisdiction-specific requirements to all negotiated outputs.

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads, and wherein no agent or participant receives PHI, raw identifiers, or sensitive economic attributes of any other participant.

**Claim 404.** The system of Claim 403 wherein **contract negotiation is executed via zero-knowledge bargaining using encrypted cost, preference, forecasting, or risk indicators.**

**Claim 405.** The system of Claim 403 wherein **marketplace optimization includes multi-criteria selection balancing cost, safety, timeliness, environmental impact, workload, or fairness constraints.**

**Claim 406.** The system of Claim 403 wherein **the contracting engine auto-generates value-sharing or settlement terms using tokenized contribution and attribution scores.**

**Claim 407.** The system of Claim 403 wherein **federated offer–response mechanisms include auction mechanisms, multi-agent bidding, matching markets, or dynamic price-discovery logic.**

**Claim 408.** The system of Claim 403 wherein **negotiated outcomes are logged as immutable Trust Blocks documenting provenance, obligations, rights, and computational scope.**

**Claim 409.** The system of Claim 403 wherein **routing decisions incorporate encrypted environmental, supply-chain, clinical, financial, or behavioral-context indicators.**

**Claim 410.** The system of Claim 403 wherein **compliance verification includes regulatory, contractual, clinical, safety, or fiduciary rules encoded as Trust Criteria.**

## Family 22.3 — Distributed Multi-Agent Governance, Oversight & Self-Correcting Economic Systems

This family protects the governance, oversight, fairness, adjudication, and dynamic self-correction mechanisms needed for safe, large-scale autonomous agent ecosystems.

These mechanisms ensure that multi-agent economies remain lawful, fair, safe, and aligned with human objectives — using encrypted context, zero-knowledge evidence exchange, and jurisdiction-aware governance structures.

The claims establish the core control plane for self-governing agent populations across clinical, financial, enterprise, logistics, and public-sector environments.

**Licensing Value:** Covers governance-supervised autonomous agent populations — including oversight, adjudication, arbitration, fairness enforcement, rule-updating, and self-correcting ecosystem dynamics. Foundational IP for safe global agent economies.

**Claim 411.** A system comprising, in any operable combination, one or more of:

**(a)** a **distributed governance engine** evaluating agent actions, proposals, allocations, or negotiations under multi-party Trust Criteria;

**(b)** an **oversight module** computing fairness, equity, safety, or compliance scores using privacy-preserved indicators;

**(c)** a **self-correction subsystem** automatically adjusting agent incentives, permissions, priorities, or routing logic when deviations or inefficiencies are detected;

**(d)** an **arbitration engine** resolving conflicts, disputes, or competitive claims among agents using encrypted or privacy-bounded context; and

**(e)** a **rule-updating and propagation layer** distributing revised governance rules, Trust Criteria, or safety parameters to agents across the ecosystem.

**Wherein** the system executes within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads, and wherein governance enforcement occurs without revealing any participant's underlying data.

**Claim 412.** The system of Claim 411 wherein **governance actions include approval, denial, throttling, escalation, or conditional-permission outcomes.**

**Claim 413.** The system of Claim 411 wherein **fairness scoring incorporates encrypted demographic, behavioral, clinical, contextual, or environmental indicators without exposing sensitive attributes.**

**Claim 414.** The system of Claim 411 wherein **self-correction includes incentive realignment, privacy-bounded nudging, allocation-path restructuring, or penalty assignment.**

**Claim 415.** The system of Claim 411 wherein **arbitration includes zero-knowledge evidence exchange, privacy-bounded reasoning, or adversarial-resilience evaluation.**

**Claim 416.** The system of Claim 411 wherein **rule updates include jurisdiction-specific, safety-specific, contractual, or multi-stakeholder requirements enforced via Trust Blocks.**

## GROUP 23 — Global Scaling, Viral Replication & Mass Adoption Mechanism (Claims 417-445)

### Family 23.1 — Accelerator-Driven Replication & Multi-Sector Scaling Architecture

This family covers the mechanisms by which QPN-enabled infrastructures replicate across enterprises, regions, sectors, and national ecosystems through accelerator-driven deployment patterns. It protects viral duplication cycles, cross-sector reuse, dual-use infrastructure leverage, plug-and-play integration via Privacy Domains, and automated instantiation of Personal and Enterprise Privacy Networks based on existing service relationships. These claims secure the growth architecture that enables mass adoption with near-zero marginal deployment cost.

**Licensing Value:** These claims are exceptionally high-value for hyperscalers, global integrators, national health systems, consumer platforms, and governments seeking to deploy QPN as a foundational privacy layer. They are required for any viral or accelerator-mediated global rollout of privacy-preserving AI, healthcare modernization, digital-public-infrastructure, or self-funding national networks.

**Claim 417.** A system comprising, in any operable combination, one or more of:

**(a)** a **replication engine** configured to instantiate new Privacy Domains, Quantum Privacy Cells (QPCs), Personal Privacy Networks (PPNs), or Enterprise Privacy Networks (EPNs) based on existing account relationships, service-provider integrations, or accelerator participation;

**(b)** an **accelerator-driven deployment module** distributing standardized Trust Criteria, Trust Blocks, governance templates, and workflow specifications across multiple organizations or sectors;

**(c)** a **viral adoption mechanism** enabling individuals, enterprises, or platforms to propagate QPN-enabled capabilities to affiliated users, customers, members, employees, or partners;

**(d)** a **dual-use infrastructure layer** allowing QPN workflows to run on existing cloud services, enterprise systems, consumer apps, financial rails, or public-sector networks without backend modifications; and

**(e)** a **cross-sector replication** controller coordinating standardized rollout patterns across healthcare, finance, public health, e-commerce, transportation, education, and government ecosystems.

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads, and wherein each replicated instance inherits privacy, security, and policy constraints without requiring centralized control.

**Claim 418.** The system of Claim 417 **wherein viral adoption is triggered automatically when a participant interacts with a QPN-enabled workflow, resulting in automatic instantiation of a PPN or EPN for that participant.**

**Claim 419.** The system of Claim 417 wherein **the replication engine provisions Privacy Domains using minimal-disclosure onboarding, zero-knowledge identity validation, or encrypted eligibility checks.**

**Claim 420.** The system of Claim 417 wherein **accelerator templates include legal, technical, governance, contractual, or regulatory-ready configurations enabling turnkey deployment in new jurisdictions.**

**Claim 421.** The system of Claim 417 wherein **dual-use infrastructure supports real-time activation of safety, payment, research, or behavioral-health workflows without modifying underlying platforms.**

**Claim 422.** The system of Claim 417 wherein **cross-sector replication includes automated propagation of privacy-preserving workflows to supply-chain partners, financial contributors, care networks, or public agencies.**

**Claim 423.** The system of Claim 417 wherein **replication cycles are logged as Trust Blocks documenting provenance, obligations, jurisdictional constraints, and cross-sector inheritance.**

## Family 23.2 — Viral Network Effects & Self-Reinforcing Adoption Dynamics

This family protects the viral economic and behavioral mechanisms by which QPN-enabled drive accelerating adoption as more participants join QPN-enabled networks. It captures cross-participant reinforcement loops, compounding value signals, multi-stakeholder benefit alignment, and the automatic formation of new Privacy Domains as network interactions deepen. These claims secure the core “network effects engine” underlying nationwide and global scaling.

**Licensing Value**: High-value for hyperscalers, digital platforms, national health systems, and consumer ecosystems. Any entity attempting to grow a trust-preserving network through viral, compounding, or self-reinforcing adoption will require a license.

**Claim 424.** A system comprising, in any operable combination, one or more of:

**(a)** a **viral-engagement engine** generating incremental value for each user interaction, thereby incentivizing additional users, enterprises, or devices to join the network;

**(b)** a **cross-participant reinforcement module** propagating improved personalization, safety, financial optimization, or service-matching accuracy as more participants contribute encrypted signals;

**(c)** an **incentive-coupling subsystem** aligning the economic, clinical, behavioral, or operational benefits of one participant with those of others;

**(d)** an **automatic PPN/EPN instantiation mechanism** triggered by user actions, service use, benefit enrollment, device pairing, clinical events, or public-health workflows; and

**(e)** a **compounding-value engine** computing marginal increases in accuracy, efficiency, safety, affordability, or convenience as network size increases.

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads, and wherein network effects accrue without exposing PHI or identifiable attributes among participants.

**Claim 425.** The system of Claim 424 wherein **engagement-triggered instantiation creates durable Privacy Domains for individuals who were not previously network participants.**

**Claim 426.** The system of Claim 424 wherein **reinforcement is driven by zero-knowledge improvements in risk prediction, eligibility detection, care personalization, economic optimization, or safety insights.**

**Claim 427.** The system of Claim 424 wherein **cross-participant incentives include financial rewards, savings redistribution, benefit enhancements, pathway optimization, or shared-value attribution.**

**Claim 428.** The system of Claim 424 wherein **viral growth includes propagation across families, workplaces, communities, clinical networks, employer groups, payer ecosystems, and public-sector programs.**

**Claim 429.** The system of Claim 424 wherein **compounding value is computed using privacy-preserved incremental-accuracy metrics or encrypted efficiency-gain indicators.**

**Claim 430.** The system of Claim 424 wherein **network effects are logged as Trust Blocks capturing provenance, contributions, dependencies, and multi-stakeholder benefit attribution.**

## Family 23.3 — Cross-Border, Cross-Jurisdiction Replication & Compliance Propagation

This family covers the mechanisms by which QPN-enabled systems replicate across states, countries, regulatory environments, and institutional boundaries while automatically inheriting and enforcing the correct legal, contractual, and jurisdictional constraints. It protects the architecture enabling global-scale rollout without duplicating infrastructure, violating privacy laws, or requiring cross-border data transfers.

**Licensing Value**: High-value IP for multinational health systems, global digital platforms, cross-border insurers, international research consortia, and governments. Any entity deploying a privacy-preserving network across jurisdictions requires these mechanisms.

**Claim 431.** A system comprising, in any operable combination, one or more of:

**(a)** a **jurisdiction-differentiation engine** determining applicable regulatory, contractual, clinical, or safety constraints based on the location of participants, systems, or workflows;

**(b)** a **compliance-propagation module** automatically attaching jurisdiction-specific obligations to data, Trust Blocks, and computational outputs;

**(c)** a **cross-border replication engine** enabling the system to instantiate new Privacy Domains and QPC clusters in foreign jurisdictions without transferring PHI across borders;

**(d)** a **constraint-harmonization layer** reconciling conflicting local, state, national, or international requirements using machine-interpretable Trust Criteria; and

**(e)** a **sovereign-computation subsystem** ensuring that computation involving foreign data executes locally within jurisdiction-appropriate Privacy Domains.

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads, and wherein cross-border scaling occurs without exporting PHI or violating data-sovereignty requirements.

**Claim 432.** The system of Claim 431 wherein **regulatory constraints include HIPAA, GDPR, 42 CFR Part 2, state privacy statutes, financial-services rules, employment protections, or international data-sovereignty laws.**

**Claim 433.** The system of Claim 431 wherein **constraint harmonization is executed using zero-knowledge reconciliation logic that avoids revealing conflicting jurisdictional attributes.**

**Claim 434.** The system of Claim 431 wherein **cross-border replication triggers automatic generation of QPCs, Trust Blocks, and policy bundles customized to the importing jurisdiction.**

**Claim 435.** The system of Claim 431 wherein **sovereign computation includes evaluation of safety, eligibility, risk, or economic indicators without exporting any underlying PHI.**

**Claim 436.** The system of Claim 431 wherein **compliance propagation includes inheritance of obligations, safety constraints, and regulatory duties from upstream data sources.**

**Claim 437.** The system of Claim 431 wherein **computational outputs destined for foreign jurisdictions are privacy-bounded, zero-knowledge summaries rather than identifiable datasets.**

## Family 23.4 — Ultra-Rapid System Instantiation, Duplication & Ecosystem Bootstrapping

This family protects the mechanisms that allow QPN-enabled systems to be instantiated, duplicated, or bootstrapped at scale — across enterprises, sectors, jurisdictions, and partner networks — without requiring traditional integrations, data migrations, or multi-year IT deployments. It covers "viral replication" of QPC-bounded infrastructures, automated ecosystem assembly, and rapid activation using existing devices, apps, platforms, and cloud services.

**Licensing Value**: Extremely high-value IP for hyperscalers, integrators, national health systems, global platforms, and multinational consortia. Any large-scale QPN deployment — healthcare, finance, government, logistics, safety, AI governance, or public health — will require these replication and bootstrapping mechanisms.

**Claim 438.** A system comprising, in any operable combination, one or more of:

**(a)** an **auto-instantiation engine** generating new QPCs, Privacy Domains, or workflow threads on demand without manual provisioning;

**(b)** a **duplication module** cloning policy sets, Trust Blocks, permission bundles, or workflow templates for new participants, institutions, or jurisdictions;

**(c)** a **bootstrap-orchestration layer** activating system capabilities using existing devices, enterprise systems, consumer apps, or platform accounts without backend changes;

**(d)** a **zero-integration activation engine** enabling immediate participation through session wrapping, interface interception, or API-independent binding; and

**(e)** a **propagation subsystem** distributing updates, rules, Trust Criteria, and safety constraints network-wide through cryptographically verifiable channels.

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads, and wherein ecosystem instantiation occurs without enterprise integrations, data transfer, or identity federation.

**Claim 439.** The system of Claim 438 wherein **auto-instantiation includes instant creation of personal, enterprise, or device-specific Privacy Domains upon first interaction.**

**Claim 440.** The system of Claim 438 wherein **duplication includes inheritance of safety rules, regulatory constraints, contractual obligations, or jurisdiction-specific logic.**

**Claim 441.** The system of Claim 438 wherein **bootstrap orchestration enables nationwide activation through existing EHR portals, consumer apps, payer portals, PBM dashboards, employer platforms, or telehealth systems.**

**Claim 442.** The system of Claim 438 wherein **zero-integration activation includes screen-wrapping, data-plane interception, event-stream relaying, or session binding.**

**Claim 443.** The system of Claim 438 wherein **propagation includes cryptographically signed distribution of governance updates, emergency safety parameters, rule changes, or threat-mitigation protocols.**

**Claim 444.** The system of Claim 438 wherein **new ecosystem participants inherit Trust Criteria automatically without manual configuration.**

**Claim 445.** The system of Claim 438 wherein **bootstrapping includes activation of multi-party workflows such as referrals, prior authorization, safety checks, research matching, or financial settlement.**

## GROUP 24 — Viral User-level, Community-level & Market-level Adoption Mechanisms (Claims 446-468)

### Family 24.1 — Viral User Activation & Peer-Propagation Mechanisms

This family protects the mechanisms through which personalized, patient-controlled Privacy Domains propagate organically through user referrals, care-team sharing, family caregiver networks, and community-based activation flows. It secures every “viral rail” that enables PPN-to-PPN onboarding, peer-to-peer trust transfer, delegated setup, caregiver-assisted enrollment, and clinician-mediated activation. The inventions covered here are foundational to mass adoption: any large-scale consumer, clinical, employer, public-health, or platform deployment of QPN must rely on some combination of these propagation mechanisms.

**Licensing Value:** Any hyperscaler, digital-health platform, employer, payer, or government attempting population-scale onboarding will require these viral rails. This family bars

competitors from replicating peer-activation loops, caregiver-mediated onboarding, clinician bootstrapping, delegated identity seeding, family-unit propagation, and similar self-replicating adoption patterns.

**Claim 446.** **A system comprising, in any operable combination, one or more of:**

**(a)** a **viral-activation interface** enabling a first user's PPN to invite, activate, or bootstrap a second user's PPN through privacy-preserved referral links, zero-knowledge eligibility checks, or delegated trust-seeding;

**(b)** a **peer-propagation engine** routing activation messages, caregiver invitations, clinician onboarding requests, or family-network enrollment tasks without exposing PHI or personal identifiers;

**(c)** a **privacy-bounded bootstrap module** enabling new users to inherit or clone non-identifying Trust Criteria, safety rules, benefit-eligibility logic, or engagement pathways from an activating user;

**(d)** a **multi-role activation subsystem** supporting parent-child, caregiver-patient, clinician-patient, employer-employee, or peer-peer onboarding without centralizing identity or clinical context; and

**(e)** an **interest-graph propagation engine** computing context-aware activation nudges using encrypted lifestyle, behavioral, or engagement indicators without exposing underlying data.

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads, and wherein viral activation occurs without transmitting PHI, raw identifiers, or re-identifiable metadata between participants.

**Claim 447.** The system of Claim 446 wherein **activation invitations are delivered using zero-knowledge proofs of relevance, eligibility, or shared-benefit without exposing contextual indicators.**

**Claim 448.** The system of Claim 446 wherein **a caregiver or clinician can pre-configure a new user's PPN with safety rules, access constraints, or engagement pathways without receiving or storing patient-controlled data.**

**Claim 449.** The system of Claim 446 wherein **activation flows include multi-party onboarding sequences involving clinicians, caregivers, family members, community organizations, or employers, each operating under independent Trust Criteria.**

**Claim 450.** The system of Claim 446 wherein **peer-propagation includes device-assisted seeding, QR-based activation, proximity-based pairing, or context-aware sharing governed by Trust Blocks.**

**Claim 451.** The system of Claim 446 wherein **inherited or cloned Trust Criteria automatically exclude any patient-identifiable data and carry forward only rights, obligations, and policy constraints.**

## Family 24.2 — Community-Level Adoption, Group Enrollment & Social-Graph Propagation

This family protects the mechanisms that allow QPN to expand through natural community structures: churches, schools, workplaces, social groups, neighborhoods, unions, digital communities, and civic organizations. It covers how entire communities adopt PPNs and EPNs through delegated verification, multi-party onboarding, anonymous network seeding, and privacy-bounded social-graph propagation. These mechanisms are crucial to viral, bottom-up growth at scale and provide an adoption moat: no competitor can replicate community-based propagation without infringing.

**Licensing Value:** Essential for any national-scale rollout involving employers, school districts, churches, unions, public programs, neighborhood health initiatives, Medicaid plans, or community-health worker ecosystems. Also critical for digital community platforms (Meta, Discord, Snap, TikTok, Reddit, etc.) that may want to use QPN for health, safety, or AI-governance features.

**Claim 452.** **The system comprising, in any operable combination, one or more of:**

**(a)** a **community-enrollment engine** enabling churches, schools, employers, neighborhood groups, or digital communities to activate PPNs or EPNs for their members without receiving PHI or identity attributes;

**(b)** a **privacy-preserved social-graph propagation subsystem** computing encrypted or zero-knowledge indicators of affiliation, proximity, shared risk, shared benefit, or group-level eligibility;

**(c)** a **delegated-verification module** enabling authorized community leaders, organizers, or systems to verify membership or role without accessing underlying personal data;

**(d)** a **multi-party onboarding workflow** that coordinates activation across clinicians, caregivers, employers, community health workers, or public-benefit organizations while preserving patient anonymity; and

**(e)** a **community-safety activation layer** that distributes group-level safety alerts, eligibility signals, environmental-risk notifications, or preventive prompts using privacy-preserved indicators.

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads, and wherein no community entity gains access to PHI, raw identifiers, or sensitive metadata of individual participants.

**Claim 453.** The system of Claim 452 wherein **community enrollment includes zero-knowledge confirmation of household membership, caregiver relationships, school enrollment, employment status, or community-group affiliation.**

**Claim 454.** The system of Claim 452 wherein **the social-graph propagation subsystem identifies multi-user activation opportunities using encrypted behavioral, environmental, or engagement indicators.**

**Claim 455.** The system of Claim 452 wherein **delegated verification is implemented through community-leader QPCs that inherit Trust Criteria preventing storage or disclosure of identifiable participant information.**

**Claim 456.** The system of Claim 452 wherein **onboarding workflows automatically tailor activation sequences based on encrypted group-level characteristics such as demographics, geography, social determinants, or risk profiles.**

**Claim 457.** The system of Claim 452 wherein **the community-safety activation layer disseminates preventive or risk-mitigating signals without revealing individual-level data.**

## Family 24.3 — Market-Level Multipliers, Network Effects & Accelerator-Driven Adoption Loops

This family protects the mechanisms by which entire markets adopt QPN/PNX simultaneously: retail, banking, transportation, education, entertainment, enterprise SaaS, healthcare, government benefit systems, and more. It covers accelerator-driven replication, cross-platform embedding, multi-sector bootstrapping, and economic incentives that amplify adoption automatically across sectors.

**Licensing Value:** Critical IP for any hyperscaler, national health plan, federal agency, state exchange, employer ecosystem, fintech platform, or global integrator attempting cross-sector deployment. Locks down market-level replication and multi-ecosystem scaling pathways.

**Claim 458.** **The system comprising, in any operable combination, one or more of:**

**(a)** a **market-activation engine** coordinating mass onboarding across sectors including healthcare, finance, retail, transportation, education, and digital entertainment without centralizing identities or PHI;

**(b)** an **accelerator-replication subsystem** enabling PPN/EPN deployment through partner networks, reseller ecosystems, integrators, community-health organizations, or large employer groups;

**(c)** a **cross-sector bootstrapping module** computing encrypted interdependency indicators that trigger adoption in adjacent markets based on observed benefit in initial sectors;

**(d)** a **marketplace-level incentive layer** distributing tokenized or contractual benefits to participants who adopt or propagate QPN capabilities; and

**(e)** a **sector-gradient engine** identifying high-leverage "activation frontiers" and prioritizing expansion paths using encrypted behavioral, economic, or epidemiologic indicators.

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads, and wherein all cross-sector activation occurs without exposing identifiable data to any participating sector.

**Claim 459.** The system of Claim 458 wherein **the accelerator-replication subsystem auto-generates deployment templates, configuration profiles, or Trust Criteria packets that can be cloned into new organizations.**

**Claim 460.** The system of Claim 458 wherein **the cross-sector bootstrapping module detects encrypted indicators of value transfer—such as reduced claims, improved safety, decreased absenteeism, or better medication adherence—to trigger propagation.**

**Claim 461.** The system of Claim 458 wherein **the incentive layer computes contribution scores and distributes value through tokenized attribution mechanisms.**

**Claim 462.** The system of Claim 458 wherein **sector-gradient prioritization includes multi-criteria assessment of impact potential, readiness, risk, adoption friction, and network leverage.**

## Family 24.4 — Viral Replication Protocols, Cross-Border Scaling & Autonomous Ecosystem Expansion

This family secures the mechanisms that allow QPN/PNX to replicate internationally, across jurisdictions, regulatory boundaries, trust frameworks, language environments, and economic systems—using automated trust inheritance, policy translation, and self-deploying privacy infrastructure.

**Licensing Value:** Essential for global scaling by Microsoft, Meta, Google, Apple, Amazon, Oracle, Cerner, Epic, McKinsey/Accenture, and sovereign public-health or digital-identity programs. This is the IP moat for *international* adoption.

**Claim 463.** **The system comprising, in any operable combination, one or more of:**

**(a)** a **jurisdictional-translation engine** converting Trust Criteria, safety rules, contractual obligations, identity frameworks, or regulatory requirements into equivalent constraints in a second jurisdiction;

**(b)** an **autonomous replication module** deploying PPNs/EPNs across borders using privacy-preserved activation loops and zero-knowledge compliance verification;

**(c)** a **cross-border propagation subsystem** detecting cryptographically protected indicators of demand, risk, compatibility, or multi-market relevance;

**(d)** a **self-configuring trust-inheritance mechanism** that automatically adapts constraints for new languages, regulatory schemes, cultural norms, or institutional environments; and

**(e)** a **global-scaling orchestration engine** managing phased rollout across markets using encrypted environmental, epidemiologic, behavioral, or economic signals.

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads, and wherein cross-border expansion is executed without revealing identifiable data to foreign jurisdictions, regulators, or platform operators.

**Claim 464.** The system of Claim 463 wherein **the jurisdictional-translation engine preserves all privacy protections and creates stronger versions when local laws permit.**

**Claim 465.** The system of Claim 463 wherein **autonomous replication includes auto-deployment templates, self-initializing Privacy Domains, and cross-lingual governance inheritance.**

**Claim 466.** The system of Claim 463 wherein **cross-border propagation includes detection of encrypted demand indicators such as emerging safety risks, chronic-disease patterns, labor-market needs, or environmental hazards.**

**Claim 467.** The system of Claim 463 wherein **the global-scaling orchestration engine simulates and optimizes multiple international rollout paths in zero-knowledge form.**

## GROUP 25 — Emergent Global Behavioral Dynamics & AI-Driven Ecosystem Optimization (Claims 468-490)

### Family 25.1 — Global Emergent-Behavior Detection, Modeling & Adaptive System Steering

Modern health, economic, environmental, and behavioral systems exhibit emergent dynamics that span jurisdictions and sectors. This family protects the infrastructure that identifies cross-system patterns, models emergent constraints, and adapts incentives, workflows, or safety protocols across millions of QPC-bounded interactions—without

revealing any individual's identity. These capabilities allow the ecosystem to detect emergent risks, self-correct, stabilize, and steer societal-level behaviors in ways that are privacy-preserving and mathematically provable.

**Licensing Value:** Critical for federal agencies, hyperscalers, large employers, health systems, payers, sovereign digital-identity programs, public-health infrastructures, and any global AI platform that needs macroscale monitoring and steering functions. No competitor can legally replicate ecosystem-level emergent-behavior governance without infringing this family.

**Claim 468.** **A system comprising, in any operable combination, one or more of:**

**(a)** an **emergent-pattern detection engine** analyzing encrypted or privacy-preserved indicators from millions of QPCs to surface global-scale behavioral, epidemiologic, safety, environmental, or economic patterns;

**(b)** a **multi-domain convergence analyzer** computing cross-sector interactions—including health, financial, mobility, behavioral, environmental, or social-context linkages—in zero knowledge;

**(c)** a **predictive trajectory engine** modeling system-wide future states and ecosystem-instability risks using encrypted indicators;

**(d)** a **macroscale adaptation engine** generating system-level interventions, incentives, or policy adjustments without accessing identifiable data; and

**(e)** a **propagation-control layer** distributing adaptation signals across PPNs and EPNs using privacy-bounded routing logic.

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads, and wherein all emergentbehavior analytics occur without revealing any individual's underlying PHI, identity, or personal context.

**Claim 469.** The system of Claim 468 wherein **emergent-pattern detection includes epidemiologic drift, medication-safety instability, behavioral-health surges, environmental stress clusters, or economic fragility indicators.**

**Claim 470.** The system of Claim 468 wherein **the convergence analyzer detects encrypted interactions between clinical signals, financial strain, social determinants, mobility patterns, and environmental exposures.**

**Claim 471.** The system of Claim 468 wherein **predictive trajectories include multi-week forecasts for population risk, system load, healthcare utilization, supply-chain stresses, or safety patterns.**

**Claim 472.** The system of Claim 468 wherein **macroscale interventions include value-based nudges, incentive adjustments, activation-sequence changes, resource allocations, or safety alerts.**

**Claim 473.** The system of Claim 468 wherein **propagation-control ensures that adaptation signals reach only authorized Privacy Domains and preserve individual anonymity.**

## Family 25.2 — Global AI-Driven Optimization of Incentives, Workflows & Resource Allocation

This family protects the system that continuously optimizes global, national, regional, or sector-wide allocation of care resources, incentives, preventive interventions, economic supports, and AI-driven workflows. It enables ecosystem-wide "policy steering" without surveillance, using only zero-knowledge signals drawn from encrypted interactions across millions of people.

**Licensing Value:** Foundational IP for any multinational AI system, payer consortium, federal public-health network, global employer ecosystem, or supply-chain platform seeking to dynamically optimize resource flows while remaining privacy compliant. This is a "must license" family for population-level AI.

**Claim 474.** **A system comprising, in any operable combination, one or more of:**

**(a) a global incentive-optimization engine** computing population-level reward pathways, subsidy levels, engagement boosts, or preventive nudges using encrypted signals;

**(b) an ecosystem workflow-adjustment module** recalibrating scheduling, referrals, care routing, or benefit logic across sectors;

**(c) a resource-allocation optimizer** distributing clinical, financial, social-support, or environmental resources using zero-knowledge state evaluation;

**(d) a multi-ecosystem feedback layer** capturing privacy-preserved results from interventions and refining global optimization; and

**(e) a dynamic-equilibrium engine** maintaining ecosystem stability by adjusting incentives and workflows without revealing individual-level data.

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads, and wherein optimization occurs without access to identity, PHI, or personal attributes of any participant.

**Claim 475.** The system of Claim 474 wherein **incentive optimization includes multi-sponsor contributions across government, employers, health plans, and community organizations.**

**Claim 476.** The system of Claim 474 wherein **workflow adjustments include cross-sector queue balancing, rerouting of high-risk cases, and dynamic assignment of preventive resources.**

**Claim 477.** The system of Claim 474 **wherein resource allocation includes cryptographically protected assessments of regional demand, social-need burden, environmental risk, or emerging safety patterns.**

**Claim 478.** The system of Claim 474 wherein **dynamic-equilibrium enforcement includes throttling, limiting, boosting, or redirecting incentives based on encrypted ecosystem stability indicators.**

## Family 25.3 — Self-Stabilizing Ecosystems, Systemic Risk Mitigation & Harm Prevention Networks

This family secures mechanisms through which QPN becomes a self-stabilizing system—automatically detecting systemic risks, dampening harmful feedback loops, preventing cascading failures, and coordinating multi-sector protective actions across millions of participants.

**Licensing Value:** Crucial for nationwide crisis-response networks, publichealth agencies, financial regulators, environmental-risk systems, supply-chain networks, and AI governance bodies. This family creates a patent moat over autonomous, privacy-preserving risk mitigation across large populations.

**Claim 479.** **A system comprising, in any operable combination, one or more of:**

**(a)** a **systemic-risk inference engine** detecting early signals of ecosystem instability using privacy-preserved inputs;

**(b)** a **cascade-prevention module** modeling risk propagation pathways and identifying nodes requiring intervention;

**(c)** a **stabilizing-intervention engine** issuing privacy-bounded actions to affected PPNs and EPNs;

**(d)** a **cross-sector protective-coordination subsystem** initiating safety measures across healthcare, finance, mobility, supply-chain, or environmental domains; and

**(e)** a **multi-level resilience engine** evaluating and strengthening system robustness over time.

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads, and wherein no systemic-risk computation requires centralizing or revealing individual-level data.

**Claim 480.** The system of Claim 479 wherein **systemic-risk inference includes detecting encrypted patterns relating to chronic-disease surges, behavioral-health**

**collapses, medication failures, environmental hazards, or financial distress.**

**Claim 481.** The system of Claim 479 wherein **cascade-prevention includes identifying highly connected nodes whose destabilization would amplify risk.**

**Claim 482.** The system of Claim 479 **wherein stabilizing interventions include targeted incentives, safety prompts, escalations, resource routing, or clinical outreach in zero-knowledge form.**

**Claim 483.** The system of Claim 479 wherein **cross-sector coordination includes privacy-preserved activation of transportation networks, food systems, supply-chain buffers, environmental monitoring, clinical-response teams, or digital platforms.**

**Claim 484.** The system of Claim 479 wherein **resilience evaluation includes encrypted multi-week predictions of system robustness, fragility, or recovery trajectories.**

## Family 25.4 — Autonomous Ecosystem Learning, Global Policy Updating & Cross-Jurisdictional Alignment

This family protects the mechanisms that allow QPN to learn from outcomes, update ecosystem-wide rules, reconcile jurisdictional differences, evolve Trust Criteria, and optimize policy parameters continuously—without exposing personal data.

**Licensing Value:** Mandatory IP for any global AI governance, national digital-policy system, or cross-border regulatory framework that needs to update policies based on encrypted real-world outcomes.

**Claim 485.** **A system comprising, in any operable combination, one or more of:**

**(a) an cryptographically-protected-outcome-learning engine** computing performance, safety, equity, or value-based results from privacy-preserved data;

**(b) a policy-optimization module** adjusting ecosystem wide rules, Trust Criteria, or safety constraints;

**(c) a jurisdictional-alignment engine** reconciling cross-border policy differences using zero-knowledge compliance verification;

**(d) a multi-stakeholder consensus layer** incorporating encrypted feedback from patients, clinicians, enterprises, and regulators; and

**(e) a continuous policy-propagation engine** distributing revised rules across PPNs and EPNs.

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v)

Trust Blocks; or (vi) EasyAccess workflow threads, and wherein no personal data is exposed during policy updating or consensus formation.

**Claim 486.** The system of Claim 485 wherein **outcome learning includes encrypted evaluation of equity, bias, access, safety, timing, throughput, adherence, or effectiveness indicators.**

**Claim 487.** The system of Claim 485 wherein **policy optimization includes automated constraint tuning, threshold adjustment, or multi-party rule harmonization.**

**Claim 488.** The system of Claim 485 wherein **jurisdictional alignment includes mapping regulatory requirements into machine-enforceable Trust Criteria.**

**Claim 489.** The system of Claim 485 wherein **multi-stakeholder consensus incorporates encrypted ballots, weighted feedback, or privacy-preserved deliberation.**

**Claim 490.** The system of Claim 485 wherein **policy propagation includes cryptographic proofs ensuring rule authenticity and preventing tampering.**

## GROUP 26 — Zero-Knowledge Credential & Identity Attestation (Claims 491-499)

### Family 26.1 — Privacy-Preserved Identity, Credential & Role Attestation

This family protects the core infrastructure for zero-knowledge identity, credential, and role attestation across healthcare, government, enterprise, public-health, clinical research, and consumer ecosystems. It enables identity-based trust without revealing underlying identifiers, preventing correlation, impersonation, surveillance, or cross-system linkage. These protections are fundamental to PPN-based clinical workflows, public-health participation, research eligibility, provider-credentialing, workforce-management, and AI-mediated patient interaction.

**Licensing Value:** This will be required by hyperscalers, digital-identity vendors, health IT platforms, zero-trust security networks, clinical-research infrastructures, and any enterprise deploying multi-party AI or cross-organizational workflows. It locks down all credentialing, licensure verification, role validation, and identity assertion flows in a QPN environment.

**Claim 491.** **A system comprising, in any operable combination, one or more of:**

**(a)** a **zero-knowledge identity-assertion module** configured to generate privacy-preserved proofs of identity, licensure, credential validity, role permissions, employment status, or professional standing;

**(b)** a **trust-verification engine** that validates identity assertions without receiving or reconstructing underlying identifiers;

**(c)** an **access-routing subsystem** that authorizes workflow participation based solely on zero-knowledge credential proofs; and

**(d)** an **impersonation-resistance module** that detects identity misuse or anomalous behavior using privacy-bounded behavioral or contextual signatures.

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads, and wherein no participant receives raw identifiers, PHI, or underlying credential details.

**Claim 492.** The system of Claim 491 wherein **identity-assertion outputs include zero-knowledge proofs of board certification, clinical privileges, employment status, enrollment status, or payer-network affiliation.**

**Claim 493.** The system of Claim 491 wherein **impersonation-resistance includes privacy-preserved behavioral signatures derived from encrypted device telemetry, workflow patterns, or interaction histories.**

**Claim 494.** The system of Claim 491 wherein **trust verification includes cross-organization credential validation without disclosing which organization issued the credential.**

**Claim 495.** The system of Claim 491 wherein **role-attestation governs access to clinical workflows, prescribing privileges, research-protocol tasks, public-health functions, or employer-authorized activities.**

**Claim 496.** The system of Claim 491 wherein **identity-assertion events are immutably recorded as Trust Blocks documenting provenance, issuance authority, validity period, and constraint inheritance.**

**Claim 497.** The system of Claim 491 wherein **access-routing uses proxy identifiers that remain cryptographically unlinkable across workflows, organizations, or jurisdictions.**

**Claim 498.** The system of Claim 491 **wherein identity proofs expire automatically unless refreshed through QPC-bound authentication using multi-factor, device-bound, or behavioral-bound signals.**

**Claim 499.** The system of Claim 491 wherein **credential proofs are used to satisfy regulatory, contractual, or clinical requirements without disclosing the underlying credential documents.**

## GROUP 26 — Privacy-Preserving Digital Twins & Predictive Simulation (Claims 500-508)

### Family 26.1 — Encrypted Digital-Twin Modeling, Trajectory Simulation & Predictive Analytics

This family secures the construction and continuous updating of encrypted "digital twins" for clinical, behavioral, environmental, and lifestyle trajectories. All modeling, simulation, and risk prediction occur within QPC-bounded domains, ensuring that no PHI, device telemetry, behavioral indicators, or contextual data are ever revealed to models, operators, researchers, or vendors. These digital twins drive the entire ecosystem of preventive care, public health, mental health, value-based contracting, and personalized benefits.

**Licensing Value:** All hyperscalers, AI model vendors, digital-therapeutic platforms, population-health networks, insurers, pharmaceutical manufacturers, and research infrastructures will need this. It forms the IP moat for encrypted simulation, predictive modeling, trajectory analysis, and risk forecasting—particularly as global healthcare moves to digital-twin-based AI.

**Claim 500.** **A system comprising, in any operable combination, one or more of:**

**(a)** a **privacy-bounded digital-twin generator** configured to create encrypted representations of clinical, behavioral, environmental, sensor-derived, or lifestyle trajectories;

**(b)** a **simulation engine** computing predictions for deterioration, improvement, relapse, instability, response-to-therapy, safety events, or environmental-risk interactions;

**(c)** a **model-recalibration engine** adjusting digital-twin parameters using encrypted updates from QPC-bound signals; and

**(d)** a **zero-knowledge output layer** providing risk scores, recommended interventions, or trajectory comparisons without exposing underlying PHI.

**Wherein** the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads, and wherein all modeling occurs without revealing source data to any model operator, platform owner, or external system.

**Claim 501.** The system of Claim 500 wherein **digital-twin updates incorporate cryptographically protected biometric, metabolic, medication-adherence, behavioral-health, or environmental-exposure indicators.**

**Claim 502.** The system of Claim 500 **wherein simulation outputs drive preventive-care nudges, clinical decision-support, benefit-design optimization, or public-health alerts.**

**Claim 503.** The system of Claim 500 wherein **trajectory forecasting includes deterioration windows, stability thresholds, relapse-risk zones, or safety-critical early-warning markers.**

**Claim 504.** The system of Claim 500 wherein **the digital-twin generator constructs multiple parallel twins representing alternative therapy paths, lifestyle interventions, or environmental conditions.**

**Claim 505.** The system of Claim 500 wherein **recalibration includes privacy-preserved gradient updates, Bayesian adjustments, reinforcement-learning refinements, or drift-correction methods.**

**Claim 506.** The system of Claim 500 wherein **multi-modal digital twins integrate encrypted clinical, behavioral, device, genomic, financial-stress, or social-determinant indicators.**

**Claim 507.** The system of Claim 500 wherein **digital-twin outputs feed value-based contracts, therapy warranties, outcome-based reimbursement systems, or safety-monitoring workflows.**

**Claim 508.** The system of Claim 500 wherein **the zero-knowledge layer restricts exposure of simulation results to only the minimal necessary outputs authorized by Trust Criteria.**