National Patient Record Repository Concept

Version 0.8

A national framework for longitudinal health information continuity

Presented by BSG, Inc.
September 2026

Document Control

Field	Value
Document	National Patient Record Repository Concept
Version	0.7
Status	Working Concept Draft for Stakeholder Review
Date	September 2026
Author	BSG, Inc.
Scope	National, participatory, and technology neutral

Version History

Version	Date	Summary
0.1	September 2026	Initial Concept baseline derived from the proposed functional architecture.
0.2	September 2026	Establishes national scope, TEFCA alignment, continuity scenario, access principles, standards positions, security posture, and Concept boundaries.
0.3	September 2026	Adds nationwide clinical-prior prefetching, authorization and audit safeguards, clinical outcomes, and requirements inherited by future documents.
0.4	September 2026	Establishes explicit protections against government overreach, insider abuse, bulk surveillance, commercial exploitation, and other foreseeable misuse; adds independent oversight, patient transparency, enforceable redress, and architecture requirements that prevent unilateral access.

Version	Date	Summary
0.5	September 2026	Establishes No Unlogged Access; distinguishes compelled disclosure, secrecy, patient-visible accounting, and internal auditing; requires immutable independent evidence, legal validation, minimization, delayed notice where permitted, and no hidden government or administrative access paths.
0.6	September 2026	Creates the Legislative Requirements Register; identifies statutory patient rights, permissible and prohibited powers, compelled-access standards, enforcement, and explicit limits applicable to every branch and level of government, the independent NPRR authority, and nongovernment actors.
0.7	September 2026	Establishes the preliminary tripartite governance model; separates policy oversight from operations; defines patient beneficial rights and NPRR fiduciary custody; permits transparent cost recovery without sale or lease of patient information; and adds funding, delegation, bankruptcy, divorce, succession, and post-death requirements to the Legislative Requirements Register.
0.8	September 2026	Adds Nationwide Autorouting Capabilities for automated delivery of studies and authorized prefetched studies

Version	Date	Summary
		to other authorized healthcare organizations, with purpose limitation, minimum-necessary routing, recipient validation, auditability, delivery controls, and downstream accountability.

Purpose of This Version

Version 0.8 adds Nationwide Autorouting Capabilities. Participating healthcare organizations may configure rules to send studies automatically to other authorized healthcare organizations and may direct authorized prefetched studies to other authorized organizations. The capability remains purpose-bound, minimum-necessary, traceable, and subject to patient authority, recipient validation, security, lifecycle, and clinical-safety controls.

Executive Summary

The National Patient Record Repository, or NPRR, is a proposed national capability that preserves and makes available a longitudinal collection of patient health information across participating United States healthcare organizations. It is intended to complement—not replace—electronic health record systems, health information networks, and the Trusted Exchange Framework and Common Agreement ecosystem.

NPRR addresses a structural weakness in healthcare today: continued availability of a patient's information often depends on the continued availability of every organization that originally created or stored it. Ransomware, infrastructure failure, natural disaster, corruption, closure, or other disruption can make essential records unavailable when care is needed most. NPRR breaks that dependency by preserving authorized information independently of the operational state of the originating organization.

NPRR is envisioned as a congressionally chartered, independently governed public-benefit organization rather than an executive-branch operating system. Its policy board would contain 27 members divided equally among government, healthcare-industry, and patient-rights groups. Each group would cast one collective vote, producing three equal votes regardless of how a group organizes internally. The board would establish policy and oversight but would not operate the repository or possess direct operational access.

Patients hold inalienable personal and beneficial rights in information maintained about them. NPRR holds the information solely as a statutory fiduciary custodian. NPRR may recover reasonable costs for authorized services, including secure research infrastructure and computing, but it may not sell, lease, pledge, or assign patient information or charge for its informational value.

The Concept is national in scope and participatory for patients and healthcare organizations. It is patient centered, standards based, resilient, technology neutral, and designed to resist misuse by government, commercial, criminal, or insider actors. FHIR is preferred for clinical-data exchange where supported and appropriate within the TEFCA and QHIN ecosystem. DICOM remains the primary interface for imaging storage and retrieval. Authorized facilities may use nationwide prefetching to obtain clinically relevant prior studies before or during care. The intended security posture references FedRAMP High, DoD Impact Level 5, and CMMC Level 2, while governance and technical controls prevent any single institution from exercising unrestricted access.

Core conclusion NPRR provides national healthcare information continuity—not merely another exchange network and not merely institutional backup.

Purpose

This Concept establishes a common understanding of the problem NPRR addresses, the value it provides, the principles that govern it, and the capabilities that belong within its conceptual scope. It provides the policy and mission foundation for a subsequent Proposal, Detailed Architecture, and supporting documents.

The Concept does not select a vendor, hosting model, database, cloud, product, network technology, or physical architecture. Those decisions must follow approval of the mission, governance principles, requirements, and program approach.

Problem Statement

Patient information is fragmented among hospitals, physician practices, laboratories, imaging facilities, pharmacies, public-sector systems, and other healthcare organizations. A patient may receive care from many organizations over a lifetime, each using local identifiers, access practices, record formats, and infrastructure.

This fragmentation makes it difficult to assemble a complete record at the point of care and to identify relevant prior studies before a scheduled examination or treatment encounter. It also creates availability risk. When an originating organization is unavailable, an otherwise authorized clinician or patient may be unable to retrieve information even when copies could have been preserved elsewhere.

Existing exchange mechanisms improve connectivity, but connectivity alone does not guarantee durable preservation, national identity correlation, recovery of lost organizational data, or continuing access when the original source is offline. NPRR is intended to provide that additional continuity layer.

Vision and Guiding Principles

1. **National scope.** NPRR serves healthcare information generated by participating civilian, commercial, nonprofit, academic, tribal, state, local, and federal sources throughout the United States.
2. **Patient centered access.** Once appropriately identified, patients retain continuing access to their own information and may authorize organizations or individuals to access it, subject to applicable law and policy.
3. **Healthcare information continuity.** The availability of preserved patient information must not inherently depend on the originating organization remaining operational.
4. **Participation and collaboration.** Participation by patients and healthcare organizations is encouraged but not mandated. Broader participation increases the completeness and resilience of the national capability.
5. **Standards based interoperability.** NPRR participates in established national exchange mechanisms and uses recognized healthcare standards.
6. **Security and trust.** Strong identity, authorization, auditing, confidentiality, integrity, availability, and governance are foundational rather than supplemental.
7. Resistance to abuse and overreach. NPRR must prevent unrestricted, secret, or purpose-free access and must remain accountable to patients and independent oversight.
8. **Technology neutrality.** The Concept defines outcomes and capabilities without prescribing implementation products or hosting platforms.
9. **Future extensibility.** The capability should accommodate evolving clinical, research, public-health, and recovery needs without weakening patient rights or trust.

National Scope and Participation

The word national describes breadth of healthcare participation and information coverage, not exclusive federal ownership or use. NPRR is not limited to the Department of Defense, Department of Veterans Affairs, federal providers, or government-generated records. Its scope includes patient information from all categories of participating United States healthcare organizations.

Participation is voluntary for patients and healthcare organizations unless future law or policy establishes a different requirement. The Concept therefore depends on clear public value, trust, workable governance, and appropriate incentives. Partial participation can still provide meaningful continuity, while broader adoption improves record completeness, identity correlation, disaster recovery, and collaboration.

Relationship to TEFCA

NPRR is the next logical extension or layer of the existing TEFCA foundation. It participates in and uses the TEFCA and Qualified Health Information Network ecosystem; it is not intended to create a competing national exchange network.

TEFCA and QHINs provide a governed framework for nationwide exchange. NPRR adds complementary capabilities centered on durable preservation, longitudinal record assembly, national identity correlation, organizational recovery, and continued authorized availability when a data-originating organization is offline.

NPRR supports TEFCA-approved exchange mechanisms. It preferentially uses standards-based FHIR for clinical-data exchange where supported and appropriate while remaining compatible with other mechanisms required for participation in the TEFCA ecosystem.

Canonical Healthcare Continuity Scenario

Hospital A Outage and Hospital B Retrieval

Hospital A has previously contributed or preserved patient information through NPRR. Hospital A's electronic health record and data services then become unavailable because of ransomware, infrastructure loss, natural disaster, data corruption, or another severe disruption.

The records already preserved in NPRR remain available. Hospital B, acting under appropriate authority, can retrieve all or an authorized subset of the Hospital A originated information through the TEFCA and NPRR ecosystem, even while Hospital A remains offline.

The authority for access must not inherently depend on Hospital A being operational at the time of the disaster. It may derive from patient authorization, previously established disaster-recovery or governance policy, applicable treatment and access rules, emergency authority, or another legally permitted basis.

> **This scenario distinguishes NPRR from ordinary source-dependent exchange: the originating organization's outage does not make the patient's preserved healthcare information unavailable.**

National Patient Identity

NPRR includes a National Patient Identifier capability and a Master Patient Index with multiple patient identifier cross-reference functions. Together, these services support reliable patient identification across independent organizations while allowing each organization to retain its internal patient identifiers.

- The NPID provides a nationally recognized identifier associated with the correctly identified patient.
- The MPI and cross-reference capability maps the NPID to authorized participating organizations' local patient identifiers.
- When authorized, cross-reference services may translate Organization A's local identifier through the NPID to Organization B's local identifier to support collaboration.
- Identity matching, identifier translation, and authorization are distinct functions. A successful identifier translation does not itself grant access to health information.

Detailed identity-proofing methods, matching algorithms, identifier formats, reconciliation procedures, and dispute-resolution workflows are deferred to later requirements, governance, and architecture work.

Longitudinal Patient Record

NPRR preserves a consolidated, longitudinal view of patient information contributed by participating sources. The record supports authorized discovery and retrieval of clinically relevant history, including automated prefetching for an anticipated episode of care. It must maintain provenance so that users can determine where information originated, when it was received, and how corrections or updates relate to prior information.

The repository complements source systems. It does not erase the responsibilities of healthcare organizations to maintain their own authoritative clinical and business records. Its national value lies in continuity, aggregation, identity correlation, authorized retrieval, and recovery.

Patient and Authorized User Access

Once appropriately identified, a patient must be able to access their own information. Patient access is a foundational property of NPRR, not a discretionary permission granted by an originating organization.

Patient authority may be exercised through a verified, purpose-limited representative, including a healthcare power of attorney or other legally recognized fiduciary. Delegation transfers authority to act within a defined scope; it does not transfer ownership or beneficial rights. Family relationship alone does not create unrestricted access.

Patients may authorize healthcare organizations or other individuals to access their information. NPRR must also recognize access permitted by applicable treatment rules, emergency authorities, disaster-recovery policies, governance decisions, and other lawful bases. The final legal and operational policy framework will define the conditions, scope, duration, delegation, revocation, and auditing of each authority.

Access decisions, including automated prefetch decisions, must use verified identity, appropriate authority, least-necessary access, traceable authorization, and comprehensive auditing. Authorization must remain enforceable during an organizational outage without silently expanding access beyond what is permitted. A general exchange relationship or successful identifier match does not create standing permission to prefetch records.

No agency, operator, administrator, funder, regulator, hosting provider, contractor, or security organization obtains unrestricted access merely because it supports or oversees NPRR. Identity correlation locates a patient record; it does not authorize a person or institution to view or use that record.

Healthcare Interoperability

Clinical Data

FHIR is the preferred standards-based mechanism for clinical-data exchange where it is supported and appropriate. NPRR remains compatible with other TEFCA-approved or required exchange mechanisms so that participation does not depend on every organization having the same technical maturity.

Imaging

DICOM is the primary and continuing interface for medical imaging storage and retrieval. It is not classified as a legacy interface and is not expected to be displaced by FHIR. FHIR may provide clinical context, orders, encounter information, or references used to identify relevant prior studies, while DICOM continues to provide the imaging-specific discovery and retrieval functions for which it is designed.

Existing Healthcare Messaging

Existing HL7-based exchange remains relevant where participating organizations or approved workflows require it. The Concept does not prescribe a forced conversion path; later requirements will define supported transactions and conformance expectations.

Nationwide Clinical Prior Prefetching

Authorized healthcare facilities may configure automated prefetch algorithms that identify and retrieve clinically relevant prior studies from participating facilities nationwide. The capability uses the NPRR and TEFCA ecosystem to discover available studies and make authorized priors available locally before or during an episode of care.

Prefetch rules may consider modality, anatomy, diagnosis, procedure, study age, scheduled encounter, and other approved clinical criteria. For imaging, DICOM remains the primary discovery and retrieval interface. FHIR and other TEFCA-supported mechanisms may supply the clinical and workflow context used to determine relevance.

Every prefetch request must have a valid authorization and purpose-of-use basis. Patient identity correlation and identifier translation help locate records but do not grant access. The service must retrieve only the minimum clinically necessary information and must prevent speculative bulk collection or retrieval unrelated to the anticipated care.

Prefetch activity must be traceable to the requesting facility, patient, purpose, authorization basis, selection criteria, source, records transferred, and disposition. Local copies remain subject to approved encryption, access, retention, caching, and deletion rules. Preserved NPRR studies may remain available for prefetch when the originating organization is offline, provided the requesting facility has authority that does not depend on the source being operational.

The intended clinical benefit is a broader inventory of historical priors for comparison at the point of care. Later documents must define measurable requirements for clinical relevance, timeliness, patient matching, false-positive and false-negative handling, authorization, audit, network and storage capacity, local lifecycle management, and clinical safety oversight.

Nationwide Autorouting Capabilities

Participating healthcare organizations may configure autorouting rules that automatically send studies to other healthcare organizations authorized to receive them. Autorouting may support established treatment relationships, referrals, transfers of care, consultations, specialist interpretation, continuity of care, and other approved clinical workflows.

A healthcare organization may also configure its nationwide prefetch rules so that studies retrieved through an authorized prefetch workflow are delivered to another authorized healthcare organization. The authority to prefetch a study does not by itself authorize forwarding it: the receiving organization, clinical purpose, information scope, and applicable patient or other lawful authorization must be validated for the routing action.

Autorouting rules must be purpose-bound, patient-specific or workflow-specific, minimum necessary, and protected against indiscriminate distribution, speculative bulk transfer, or creation of standing access between organizations. Identity correlation and identifier translation may support accurate routing but do not grant access or permission to disclose information.

Every automated routing event must be traceable to the initiating organization, responsible user or system, patient, purpose, authorization basis, routing rule, source, destination, records transferred, delivery status, and final disposition. Information received through autorouting remains subject to approved encryption, access, retention, caching, redisclosure, correction, and

deletion requirements. The receiving organization assumes accountability for its authorized local copy and may not route it onward without separate authority.

Later documents must define measurable requirements for rule governance, recipient validation, consent and authorization evaluation, patient matching, duplicate suppression, clinical relevance, delivery acknowledgment, retry and exception handling, reconciliation, audit, network and storage capacity, local lifecycle management, and clinical safety oversight.

Initial Conceptual Capabilities

- National patient identification and identity correlation
- Multiple patient identifier cross-reference

- Longitudinal health-record preservation
- Authorized clinical-record query and retrieval
- Nationwide authorized prefetching of clinically relevant prior studies
- Nationwide autorouting of studies and authorized prefetched studies among authorized healthcare organizations
- DICOM imaging storage and retrieval
- Healthcare organization backup and recovery

- Continuity access during source-system outages
- Patient access and patient-authorized sharing

- Provenance, audit, and accountability
- Misuse detection, independent oversight, patient transparency, and enforceable redress
- Consented or otherwise authorized analytics and research using appropriately protected data

Future Conceptual Capabilities

Future capabilities may include advanced analytics, appropriately governed artificial-intelligence assistance, public-health support, insurance and benefits coordination, and new national collaboration services. Inclusion in this future-looking list does not authorize deployment or data use. Each capability requires separate legal, ethical, privacy, governance, security, and program review.

Security Privacy and Trust

NPRR would hold highly sensitive health information at national scale. Its security and privacy posture must therefore be designed to meet or exceed the needs of participating patients and organizations and to support high-assurance government use where applicable.

The Concept references FedRAMP High, DoD Impact Level 5, and CMMC Level 2 as security benchmarks. These references express the intended rigor of the program; they do not select a hosting provider, assert certification before assessment, or require every participating organization to become a federal contractor.

- Strong identity proofing, authentication, authorization, and least-privilege access
- Protection of data confidentiality, integrity, and availability
- Purpose-bound controls for automated discovery, prefetching, local caching, retention, and deletion
- Comprehensive, immutable, independently reviewable, and tamper-evident audit records for every access, disclosure, privileged action, and attempted bypass
- Resilience without a single point of failure
- Separation of duties and accountable administrative access
- Protection of patient choice, consent, and legally permitted access
- Incident response, disaster continuity, and recovery
- Governance for secondary use, de-identification, research, and analytics
- No universal backdoor, master key, standing government access, classified interface, emergency account, or administrative path that bypasses normal authorization or auditing
- Data minimization, segmentation, encryption, continuous monitoring, and anomaly detection
- Independent audit evidence and patient-visible access histories where disclosure is legally and operationally safe

Foreseeable Abuse Misuse and Institutional Overreach

Why These Risks Belong in the Concept

A repository with national reach could improve continuity of care, but the same scale could magnify harm if access rules are weak, hidden, or changed without public accountability. Trust therefore depends on enforceable limits that apply to every actor, including the institutions that fund, operate, regulate, host, secure, or oversee NPRR. These limits are part of the mission and must survive changes in leadership, policy, vendor, and technical implementation.

Foreseeable Threat Actors and Abuse Scenarios

Foreseeable actors include government agencies, law enforcement bodies, immigration authorities, political officials, foreign intelligence services, organized crime, ransomware groups, data brokers, malicious vendors or contractors, privileged administrators, compromised insiders, insurers, employers, and researchers who exceed their authorization.

Unacceptable uses include:

- Surveillance, profiling, or population monitoring without a legitimate medical purpose and valid legal authority

- Identifying or penalizing people who crossed jurisdictional boundaries to obtain lawful care, including reproductive or other sensitive care
- Bulk access justified by generalized national security, law enforcement, immigration, political, or public-order claims without case-specific authority and appropriate judicial review
- Fishing expeditions, speculative searches, group profiling, re-identification, or artificial-intelligence analysis unrelated to an authorized purpose
- Commercial sale or lease of patient information; pricing based on the informational value, number, rarity, or medical significance of records; discriminatory use; unauthorized secondary use; or access by insurers or employers beyond a lawful and specifically authorized purpose
- Insider misuse, credential abuse, silent administrative access, mass extraction, ransomware, or exfiltration by criminal or foreign actors
- Mission creep that makes voluntary participation mandatory through administrative practice without transparent legal authority, public review, and effective protections

Required Safeguards

Every access must be purpose bound, limited to the minimum necessary information, time limited where appropriate, and attributable to a verified person, organization, authority, and patient context. Non-care access requires valid legal authority and appropriate judicial or independent review. Emergency access must be narrowly scoped, time limited, and fully auditable.

NPRR must prohibit speculative bulk queries and must detect unusual access patterns, mass downloads, repeated failed authorization, inappropriate cohort searches, and other indicators of misuse. Audit records must be tamper evident and independently reviewable. Patients should be able to see who accessed their information, for what purpose, and under what authority whenever disclosure is legally and operationally safe.

Administrative power must be divided through separation of duties, least privilege, dual control or multi-party authorization for exceptional actions, and independent oversight. No single institution, cloud provider, government body, operator, or administrator may be able to silently weaken protections, decrypt the repository, erase audit evidence, or grant itself broad access.

Governance must include meaningful representation for patients, privacy and civil-liberties interests, clinicians, security and interoperability experts, participating organizations, and multiple jurisdictions. It must publish material rules, report aggregate access and enforcement activity, protect good-faith whistleblowers, provide correction and appeal processes, and impose enforceable sanctions for misuse.

Compelled Access Secrecy and Audit Integrity

Federal, state, tribal, territorial, or local authorities may seek identifiable NPRR information through warrants, subpoenas, court orders, administrative demands, healthcare-oversight authority, public-health authority, or national-security and intelligence processes. HIPAA and

related privacy rules do not create an absolute barrier to every legally compelled disclosure. NPRR must therefore distinguish legal authority to require a limited disclosure from technical authority to enter, search, or operate the repository.

> **The NPRR No Unlogged Access principle is absolute as a system and governance requirement: every human, service, administrator, operator, contractor, law-enforcement, intelligence, oversight, emergency, or automated access to patient-identifiable information must generate an immutable audit record. No actor may be provided a hidden interface, unlogged account, undocumented extraction mechanism, or privilege capable of disabling, altering, suppressing, or deleting audit evidence.**

A lawful secrecy, sealing, nondisclosure, grand-jury, or classified requirement may restrict patient notification, public reporting, or who may review an audit record for a defined period. It must not prevent the audit record from being created and preserved under independent control. Patient-visible disclosure accounting is distinct from internal security auditing: an access may be temporarily withheld from the patient where law requires, but it may not be technically unaudited.

Compelled requests must be received and validated through a dedicated legal-response process. NPRR must verify jurisdiction, legal sufficiency, scope, patient population, purpose, and duration; challenge defective, vague, bulk, politically motivated, or overbroad demands to the maximum lawful extent; disclose only the specifically required minimum information; and prevent the requesting authority from receiving standing credentials or direct repository access. Delayed patient notice and audit visibility must occur when the restriction expires or disclosure becomes lawful.

Because information might also be sought from a hosting provider, network operator, backup custodian, participating organization, endpoint, or replicated system, later architecture and contracting must ensure that audit evidence is generated across every layer under NPRR control. Cryptographic verification, independently controlled logging, separation of duties, multi-party approval, key-control separation, aggregate transparency reporting, and external oversight must make covert or unilateral access difficult to conduct and difficult to conceal.

NPRR cannot guarantee that a future law, binding court order, physical seizure, covert compromise, or sovereign action will never result in government access. Its enforceable commitment is that it will contain no designed mechanism for silent or unaccountable access, will preserve evidence of every access within its control, will minimize and contest compelled disclosure where legally supportable, and will provide eventual accountability whenever law permits.

Requirements for Later Documents

The Proposal, Detailed Architecture, security plans, governance policies, and operating procedures must convert these protections into measurable requirements. Architecture work must evaluate distributed or federated control, independently controlled cryptographic keys, hardware security modules, split-key or quorum approval, confidential computing, zero-trust access, immutable external audit records, segmented data, independent monitoring, offline recovery, and portability between providers. These are required design considerations, not a decision for a particular cloud, vendor, or deployment model.

The safety of cloud, on-premises, hybrid, or multi-provider deployment depends more on governance, control separation, key ownership, monitoring, and recoverability than on location alone. Later design decisions must reduce dependence on any single provider or government and must not introduce a universal access mechanism.

Governance Principles

NPRR requires trusted national governance that represents patients, healthcare organizations, exchange participants, public-sector stakeholders, security and privacy interests, and other affected communities. Governance must define accountability without converting this Concept into a product design.

Preliminary Governing Board Structure

The preliminary model is a 27-member policy board divided into three groups of nine members each: government, healthcare industry, and patient rights. Each group casts exactly one collective vote. The governing body therefore has three equal votes, and no group gains additional voting power because of its membership count, internal structure, funding contribution, or operational role.

The government group must represent all three constitutional branches. Judicial representation need not be provided by active judges and may include retired judges or other qualified representatives of the judicial branch. The detailed appointment method, qualifications, terms, removal protections, ethics requirements, and internal voting procedures remain to be developed.

The healthcare-industry group should include healthcare institutions and healthcare providers and may include private insurers, electronic health record companies, picture archiving and communication system companies, medical-device or pharmaceutical manufacturers, and other

materially affected healthcare-technology organizations. Its internal allocation must prevent any single industry segment from dominating the group.

The patient-rights group must consist of independent fiduciaries whose primary duty is to protect patients and patient rights. Members may not serve merely as representatives of government, industry, employers, insurers, data brokers, or NPRR operators. Independence, conflicts, funding, selection, removal, and accountability requirements must be defined in the charter and implementing legislation.

The board establishes policy, approves governance standards, oversees compliance, and appoints or removes accountable executive leadership as authorized by statute. It has no operational control over production systems, patient records, access approvals, credentials, encryption keys, audit logs, or individual disclosure decisions. Operations must be performed by separately accountable management under published policy, separation of duties, and independent audit.

- Transparent policies for participation, access, contribution, correction, and withdrawal
- Patient representation and accessible dispute and redress processes
- Clear allocation of stewardship, operational, oversight, and enforcement responsibilities
- Rules for prefetch eligibility, clinical relevance, purpose of use, local retention, patient transparency, and misuse prevention
- Rules for emergency and disaster operation that exist before an outage occurs
- Alignment with applicable federal, state, tribal, and healthcare-sector obligations
- Measurable accountability for security, availability, interoperability, and patient outcomes
- Independent oversight with patient, clinical, privacy, civil-liberties, technical, and multi-jurisdiction representation
- Published rules, aggregate transparency reporting, whistleblower protection, enforceable penalties, and accessible correction and appeal
- A transparent change process that prevents silent weakening of patient rights or conversion of voluntary participation into a mandate

Ownership Funding and Fiduciary Custody

Organizational Form and Funding

The preliminary ownership model is a congressionally chartered, independently governed nonprofit public-benefit NPRR Authority. It is not owned or operated by an executive agency, healthcare company, insurer, technology vendor, or patient-data investor. Government funding may provide the primary financial foundation, including a durable statutory trust fund or multiyear appropriation, but funding does not confer access, operational control, additional votes, or authority to weaken auditing and patient protections.

Funding may combine protected public appropriations, participant or service fees, grants, and other charter-authorized revenue. Financial sources must be disclosed and governed by conflict rules. No contributor may purchase preferential access, approval, governance influence, exclusivity, or reduced oversight. Detailed funding formulas, capitalization, fee schedules, and transition plans remain Proposal and legislative-design matters.

Patient Data Rights

Patients hold personal and beneficial rights in information maintained about them. NPRR holds that information solely as a statutory fiduciary custodian. These rights are inalienable and may not be sold, leased, pledged, collateralized, waived through adhesion terms, divided as marital or community property, transferred in bankruptcy, reached by creditors, or treated as an asset of NPRR or any operator, participant, vendor, or successor.

A patient may grant a revocable and scope-limited agency to a verified representative. A medical power of attorney, guardian, executor, administrator, or other legally recognized representative may exercise only the authority provided by law and the governing instrument. Delegation never conveys a commercial interest or a right to sell, lease, or exploit the information.

Permissible Service and Research Fees

NPRR may charge transparent and reasonable fees for services needed to conduct an authorized activity, including application and ethics review, de-identification, secure workspace configuration, computing, storage, networking, technical support, auditing, compliance monitoring, and controlled review of research outputs. Fees compensate NPRR for services, infrastructure, reasonable overhead, and program sustainability; they do not purchase patient information or its informational value.

An approved researcher receives only purpose-bound, time-limited access in an authorized environment. Payment confers no ownership, general license, exclusivity, right of re-identification, right of downstream reuse, or entitlement to export record-level information. Fee schedules, waivers, public-interest subsidies, excess-revenue treatment, and independent financial review must be defined transparently.

Incapacity Death and Succession

During incapacity, a verified representative may exercise only the authority recognized by applicable law or a valid patient directive. NPRR must apply minimum-necessary access, purpose limitations, revocation and restoration procedures, abuse protections, and complete auditing.

At death, patient information does not become ordinary inheritable or commercially transferable property. NPRR first follows a valid patient directive or designated health-information representative. Otherwise, a legally recognized personal representative may exercise limited fiduciary authority for defined purposes such as estate administration, claims, correction, family medical-history needs, or authorized disclosure. Other heirs or relatives receive only access specifically authorized by law or the patient's directive. The duration of post-death protection, sensitive-record rules, representative priority, conflicts among claimants, and treatment when no representative exists remain legislative design items.

NPRR-held information is not an asset that can be assigned in NPRR bankruptcy, dissolution, receivership, merger, or reorganization. If NPRR ceases operation, records and fiduciary duties may pass only to a legally authorized successor custodian subject to protections at least as strong as those in the NPRR charter.

Legislative Requirements and Limits on Authority

Purpose and Continuing Status

Certain NPRR protections require federal legislation because voluntary policy, contracts, regulations, governance rules, and technical controls can be changed by the institutions they are intended to constrain. This section is the initial Legislative Requirements Register. Its identifiers must be preserved and traced through the Proposal, legislative drafting, legal analysis, Detailed

Architecture, governance instruments, security plans, operating procedures, testing, and independent audits.

The register identifies required statutory outcomes rather than final bill language. Each item remains open until qualified counsel confirms the constitutional basis, interaction with existing federal and state law, enforcement mechanism, and implementing language, and until the enacted protection is mapped to enforceable governance and technical controls.

Constitutional Boundary

Legislation can establish rights, duties, causes of action, jurisdiction, funding conditions, evidentiary standards, agency limits, preemption rules, and criminal or civil penalties. It cannot eliminate powers granted directly by the Constitution, dictate the result of a particular Article III case, or permanently prevent a future Congress from amending or repealing a statute. NPRR must therefore combine legislation with independent governance, distributed technical control, immutable evidence, public transparency, and a requirement that any material weakening occur only through visible legislative action rather than silent policy or administrative change.

Foundational Charter and Patient Rights

LEG-01 National charter and independence. Establish NPRR through a federal statutory charter defining its narrow public-healthcare-continuity mission, independent governance, enumerated powers, prohibited powers, fiduciary duties to patients, and freedom from unilateral control by any branch, agency, jurisdiction, funder, operator, or private organization.

LEG-02 Enforceable patient rights. Establish rights of authenticated access, correction, provenance, meaningful disclosure history, notice when legally permitted, authorization and revocation, appeal, redress, and recovery for violations. Define administrative remedies, judicial review, standing, and an appropriate private right of action.

LEG-03 Voluntary participation and anti-coercion. Preserve the settled participatory model; prohibit conversion to mandatory patient or organizational participation through agency practice, contract leverage, funding conditions, emergency declaration, or governance action without express and publicly enacted legislation and renewed rights review.

LEG-04 Permissible and prohibited uses. Define authorized healthcare continuity, treatment, recovery, patient-directed sharing, and specifically approved secondary uses. Prohibit purpose-free access, population surveillance, political targeting, immigration enforcement, punishment for lawful care across jurisdictional boundaries, speculative searches, discriminatory use, commercial sale, unauthorized artificial-intelligence analysis, and re-identification.

Limits on Congress and the Legislative Branch

LEG-05 Legislative-branch access. Membership in Congress, committee jurisdiction, appropriations authority, investigation, or oversight must not create direct credentials or standing access to identifiable NPRR information. Any compelled production must rest on valid constitutional and legal authority, be tied to a legitimate legislative purpose, identify a particular scope, use the minimum necessary information, undergo independent legal validation, and generate immutable audit evidence.

LEG-06 Transparent legislative change. Material expansion of NPRR powers or weakening of patient rights must require express statutory language and public legislative process. Appropriations riders, committee instructions, informal requests, funding threats, and nonpublic agreements must not silently create access or disable safeguards. This requirement cannot bind a future Congress absolutely, but it establishes the required statutory and governance defense against implied or covert expansion.

Limits on the Executive Branch

LEG-07 No executive-action-only access. An executive order, presidential directive, emergency declaration, national-security assertion, classification decision, agency policy, regulation, or enforcement priority must not, standing alone, authorize access to identifiable NPRR information. Every demand must identify separate constitutional or statutory authority and satisfy the applicable judicial or independent-review standard.

LEG-08 No unilateral executive control. The President and executive agencies must not possess unilateral authority over NPRR governance, operating credentials, cryptographic keys, decryption, authorization rules, audit evidence, patient notification, appointment and removal of all overseers, or the creation of emergency or classified access paths.

LEG-09 Executive-agency demands. Warrants, subpoenas, administrative demands, healthcare-oversight requests, public-health authorities, foreign-intelligence processes, and law-enforcement requests must be case-specific, legally validated, purpose bound, time limited where appropriate, and minimized. NPRR must have standing and resources to challenge defective, vague, bulk, politically motivated, or overbroad demands and to seek appellate review.

Limits on the Judicial Branch

LEG-10 Judicial process and particularity. Judicial office, court administration, or adjudicative interest must not create direct NPRR access. Court-authorized disclosure must use a warrant, order, subpoena, or other recognized process supported by the constitutionally and statutorily required showing, particularized scope, jurisdiction, minimization, return or destruction rules, immutable auditing, and meaningful opportunity for challenge where law permits.

LEG-11 Sealed and secret proceedings. Sealing, nondisclosure, grand-jury secrecy, and classified proceedings may delay patient notice or restrict who may review an audit record, but must not authorize unlogged access, deletion or alteration of evidence, indefinite secrecy without renewed findings, or direct court access to the repository. Legislation must provide periodic review and eventual notice when lawful.

Limits on State Local Tribal and Territorial Authorities

LEG-12 Uniform national floor and preemption. Establish a national minimum privacy and access standard while preserving stronger compatible protections. Define when federal law preempts conflicting demands, including efforts to investigate or penalize care lawfully provided in another jurisdiction, bulk population searches, and demands that evade NPRR safeguards through a participating organization or service provider.

LEG-13 No jurisdiction-based privileged access. State, local, tribal, or territorial sponsorship, licensing, funding, public-health responsibility, law enforcement, or participation must not create standing access. Valid demands remain subject to jurisdiction, case-specific authority, minimization, auditing, contestability, and applicable sovereign and constitutional limits.

Limits on the Independent NPRR Authority

LEG-14 Enumerated powers and fiduciary duty. The independent NPRR Authority must exercise only powers expressly granted by statute. It must not expand its mission; sell, lease, or monetize the informational value of patient information; create new mandatory uses; or obtain operational access merely through its oversight role. It may collect transparent, reasonable fees for charter-authorized services and infrastructure subject to statutory cost, conflict, and audit controls.

LEG-15 Distributed governance and conflicts. Require patient, clinical, privacy, civil-liberties, security, interoperability, and multi-jurisdiction representation; staggered terms; transparent appointment and removal standards; conflict-of-interest and revolving-door restrictions; public rulemaking; recorded votes; whistleblower protection; and independent review. No stakeholder class may control a majority of authorization, key, audit, or enforcement functions.

LEG-16 No self-issued immunity. The NPRR authority must not grant itself immunity, waive violations, suppress notices, settle away patient rights, or become the sole judge of its own compliance. Independent inspectors, regulators, courts, and patient remedies must remain available.

Limits on Nongovernment Organizations and Individuals

LEG-17 Operators vendors and infrastructure providers. Hosting providers, contractors, software vendors, network operators, backup custodians, certificate authorities, and security providers must have no independent right to use or disclose NPRR information. Statutory duties must follow the data and prohibit hidden access, secondary use, sale, model training, retention beyond duty, credential reuse, and compliance with demands that bypass the NPRR legal-response process.

LEG-18 Participating healthcare organizations. Contribution, treatment relationship, TEFCA participation, identity matching, prior possession, or recovery rights must not create unrestricted access. Organizations may use data only for authorized purposes and remain accountable for local copies, prefetching, redisclosure, retention, security, correction, and patient transparency.

LEG-19 Insurers employers data brokers and commercial users. Prohibit access or use for employment, underwriting, eligibility, pricing, marketing, behavioral profiling, credit, sale, or discrimination except where a narrowly defined law expressly permits a necessary transaction with appropriate patient rights and safeguards.

LEG-20 Researchers public-health users and analytics providers. Require specific legal and ethical authority, data minimization, independent review, purpose limitation, re-identification prohibitions, publication controls, time-limited access, and enforceable sanctions. Payment may cover authorized review, de-identification, secure infrastructure, computing, storage, support, audit, and compliance costs but must confer no ownership, general license, exclusivity, export right, or preferential approval.

Compelled Access Audit and Secrecy

LEG-21 No Unlogged Access in statute. Codify that every access, disclosure, administrative action, key use, export, and attempted bypass involving identifiable information creates immutable, independently controlled evidence. No government or nongovernment actor may order, request, build, or use an unlogged mechanism or require alteration, suppression, or destruction of audit evidence.

LEG-22 Time-limited secrecy and eventual notice. Require particularized findings for delayed notice, fixed expiration, periodic judicial review, aggregate transparency reporting during secrecy, and patient notice when the restriction ends or disclosure becomes lawful. Classification must not substitute for access authority or place audit evidence under exclusive control of the requesting agency.

LEG-23 Sensitive information protections. Establish heightened process and minimization for reproductive, substance-use, behavioral-health, genetic, infectious-disease, minor, sexual-health, gender-affirming-care, and other specially protected information, while preserving emergency treatment and the patient's own access.

Accountability Enforcement and Durability

LEG-24 Independent enforcement. Establish an independent inspector, civil-liberties and patient advocate, external audit authority, referral duties, judicial remedies, and meaningful civil and criminal penalties applicable to officials, directors, employees, contractors, organizations, and knowing recipients of unlawfully obtained information.

LEG-25 No immunity through office contract or funding. Government office, judicial status, legislative status, sovereign involvement, board membership, employment, contract, grant, regulation, security responsibility, or funding must not itself excuse unauthorized access or defeat applicable remedies. Final legislation must address legitimate sovereign-immunity and official-immunity doctrines expressly and constitutionally.

LEG-26 Emergency powers. Emergency access must use predefined statutory criteria, the minimum necessary scope, named accountable decision makers, immutable auditing, short automatic expiration, prompt independent review, and post-event notice. Emergencies must not create permanent authorities, population-wide access, or reusable credentials.

LEG-27 Legal harmonization. Reconcile the NPRR statute with HIPAA, the Privacy Act, substance-use confidentiality law, federal and state health-privacy laws, TEFCA obligations, electronic-communications law, foreign-intelligence authorities, public-health law, civil-rights law, evidentiary process, records-retention duties, tribal law, and state-law preemption. Where existing law permits broader access than the NPRR trust model, legislation must state the intended higher standard explicitly.

LEG-28 Funding and continuity. Provide durable public funding, including authority for a protected statutory trust or multiyear appropriations, together with transparent charter-authorized service revenue. Appropriations, grants, contracts, emergency support, or private contributions must not be conditioned on secret access, reduced auditing, additional governance votes, preferential research approval, commercial exploitation, or weakened patient rights.

LEG-29 Periodic public review. Require scheduled public review of the statute, authorities used, denied and challenged demands, secrecy duration, audit findings, sanctions, technology changes, and civil-rights effects. Review may recommend amendments but must not itself expand access without the legally required public process.

Patient Rights Governance Funding and Succession

LEG-30 Patient beneficial rights and fiduciary custody. Establish inalienable personal and beneficial rights for patients and designate NPRR as statutory fiduciary custodian rather than owner of the informational value of patient records.

LEG-31 Nontransferability in private proceedings. Exclude patient information rights and NPRR-held records from sale, lease, lien, collateral, creditor process, bankruptcy estates, and division as marital or community property. Permit only legally recognized, scope-limited agency and fiduciary authority.

LEG-32 Delegation incapacity and representation. Define verification, scope, duration, revocation, restoration of patient control, minimum-necessary access, abuse prevention, and audit requirements for healthcare powers of attorney, guardians, family designees, and other representatives.

LEG-33 Post-death stewardship. Provide a priority order for patient directives, designated health-information representatives, executors or administrators, and limited family access. Prohibit inheritance as commercially transferable property and define duration, sensitive-record treatment, conflicts, and no-representative cases.

LEG-34 Service fees and research cost recovery. Authorize reasonable, transparent, independently reviewed fees for approved services and infrastructure while prohibiting per-record pricing, sale or lease of information, value-based royalties, preferential approval, ownership transfer, re-identification, and unauthorized reuse.

LEG-35 NPRR insolvency dissolution and successor custody. Declare patient information outside the NPRR Authority's estate and prohibit transfer through bankruptcy, receivership, merger, reorganization, or dissolution except to an authorized successor fiduciary bound by equal or stronger protections.

LEG-36 Tripartite policy governance. Establish a preliminary 27-member board with nine government, nine healthcare-industry, and nine independent patient-rights members. Require one collective vote per group, representation of all three government branches, and safeguards against capture within each group.

LEG-37 Policy and operational separation. Limit the governing board to policy, oversight, compliance, and accountable leadership functions. Prohibit board members and groups from direct operational control, production credentials, patient-record access, access adjudication, cryptographic keys, or alteration or suppression of audit evidence.

LEG-38 Organizational independence and financial firewalls. Charter NPRR as an independently governed nonprofit public-benefit authority; prohibit ownership or control by an executive agency, healthcare organization, insurer, vendor, investor, or funder; and prevent financial leverage from creating access or governance privileges.

Register Governance

The Legislative Requirements Register is a controlled project artifact. New requirements receive permanent identifiers; revisions preserve history and rationale; no item is closed merely because a policy, contract, or design control partially addresses it. Closure requires enacted authority or a documented determination by qualified counsel that legislation is unnecessary, plus mapping to governance, implementation, verification, oversight, and remedy. Legal conclusions and proposed statutory text require review by qualified constitutional, healthcare-privacy, national-security, administrative-law, tribal-law, and legislative counsel as applicable.

Conceptual Scope

Included

- Mission, intended outcomes, scope, participation principles, and national value
- Relationship to TEFCA, QHINs, and recognized healthcare standards
- Patient identity, cross-reference, access, continuity, preservation, recovery, and audit capabilities
- High-level security, privacy, trust, resilience, and governance principles

Deferred

- Cloud, private data center, hybrid, or other hosting selection
- Vendors, products, databases, operating systems, and network components
- Physical and logical topology, regional design, replication, sizing, and performance engineering
- Detailed consent workflows, identity algorithms, security controls, and certification plans
- Detailed funding formulas, fee schedules, capitalization, acquisition, contracting, internal organizational structure, and operating model
- Detailed rollout schedules, migration plans, service levels, and implementation sequencing

Concept Success Outcomes

The program should ultimately be judged by outcomes rather than by the presence of a particular technology. Proposal and architecture work should establish measurable targets for the following outcomes:

- Patients can obtain their available information after reliable identification.
- Authorized care teams can retrieve necessary records across organizational boundaries.

- Preserved information remains available during an originating organization's outage.
- Organizations can recover contributed data after local loss.
- Patient identity is correlated accurately, transparently, and with effective redress.
- Access is authorized, limited, auditable, and understandable to affected patients.
- Authorized care teams receive clinically relevant prior studies in time to support comparison and treatment decisions.
- Clinical and imaging information is exchanged through appropriate national standards.

- Security and availability meet the program's stated high-assurance posture.
- No single institution can obtain unrestricted access, suppress audit evidence, or silently weaken patient protections.

Settled Concept Positions

Position	Concept Baseline
Name and scope	National Patient Record Repository covering participating U.S. healthcare information regardless of organizational origin.
Exchange relationship	Extension of and participant in the TEFCA and QHIN ecosystem, not a competing network.
Participation	Participatory for patients and organizations; organizational participation is encouraged rather than mandated.
Patient access	An appropriately identified patient retains access to their own information.
Continuity	Preserved information remains available independently of the originating organization's operational state.
Clinical exchange	FHIR preferred where supported and appropriate, with compatibility for other TEFCA-required mechanisms.
Imaging	DICOM is the primary imaging storage and retrieval interface and is not legacy.
Security posture	FedRAMP High, DoD IL5, and CMMC Level 2 are referenced as benchmarks.
Technology stance	The Concept remains technology neutral.
Clinical prior prefetching	Authorized facilities may automatically retrieve clinically relevant prior studies nationwide using purpose-bound, minimum-necessary, auditable rules.
Abuse resistance	Government, commercial, criminal, and insider access is purpose bound, minimum necessary, attributable, auditable, and subject to independent oversight; bulk surveillance and speculative population searches are prohibited.

Position	Concept Baseline
No Unlogged Access	Every access to patient-identifiable information creates immutable, independently reviewable evidence. A lawful secrecy requirement may temporarily restrict patient notification or audit visibility, but may not prevent creation and preservation of the audit record. No government, intelligence, law-enforcement, emergency, vendor, or administrator receives a hidden or unaudited access path.
Institutional control	Funding, regulation, operation, hosting, security, or oversight does not confer unrestricted access. No single institution may silently bypass authorization, decrypt the repository, erase audit evidence, or weaken patient rights.
Patient accountability	Patients receive meaningful access transparency, correction, appeal, and redress where legally and operationally possible.
Legislative protection	Patient rights and limits on every government branch, level of government, the independent NPRR authority, and nongovernment actors must be established through an identified Legislative Requirements Register and traced into enacted law, governance, implementation, oversight, and remedies.
Governing board	Preliminary 27-member board: nine government, nine healthcare-industry, and nine independent patient-rights members.
Equal voting	Each of the three groups casts one collective vote; there are three equal votes regardless of internal organization.
Government representation	The government group represents all three branches; judicial representation may include retired judges or other qualified branch representatives.
Board authority	The board establishes policy and oversight but has no operational control, production access, access-approval role, cryptographic keys, or

Position	Concept Baseline
	authority to alter audit evidence.
Patient data rights	Patients hold inalienable personal and beneficial rights; NPRR holds information solely as statutory fiduciary custodian.
No sale or lease	NPRR may not sell, lease, pledge, collateralize, or assign patient information or monetize its informational value.
Service cost recovery	NPRR may charge transparent, reasonable fees for authorized review, de-identification, secure infrastructure, computing, storage, support, audit, and compliance services.
Private proceedings	Patient information rights and NPRR-held records are not divisible in divorce, transferable in bankruptcy, reachable by creditors, or assets of NPRR.
Delegated authority	A verified medical power of attorney or other lawful representative receives purpose- and scope-limited authority, never ownership or commercial rights.
Post-death stewardship	Rights do not pass as ordinary inheritable property; patient directives control first, followed by limited authority for a legally recognized personal representative.
Organizational model	Preliminary model is a congressionally chartered, independently governed nonprofit public-benefit NPRR Authority.
Funding	Primary public funding may be supplemented by protected service fees and grants; funding never confers access, control, extra votes, or reduced oversight.

Items for Proposal and Later Work

The following matters are intentionally not resolved in this Concept. They form the starting agenda for the Proposal, Detailed Architecture, and supporting documents.

- Appointments, qualifications, terms, removal, ethics, conflicts, and internal procedures for the three governing groups; accountable executive management; operational staffing; and independent oversight implementation
- Participation incentives, onboarding, and phased adoption
- Detailed legal and policy framework for consent, treatment, emergency, disaster, revocation, representation, incapacity, post-death stewardship, and secondary use
- NPID issuance, identity proofing, matching, reconciliation, and dispute resolution
- Record retention, correction, provenance, legal hold, archival, and deletion rules
- Nationwide prefetch and autorouting governance, authorization, relevance and routing rules, recipient validation, patient matching, clinical safety, audit, delivery assurance, local-copy lifecycle, and performance requirements
- TEFCA and QHIN operational responsibilities and supported exchange workflows
- Implementation architecture, hosting, regionalization, capacity, performance, and service levels
- Security-control implementation, assessment, authorization, monitoring, and incident response
- Formal abuse-case threat model covering institutional overreach, insider misuse, bulk surveillance, commercial exploitation, re-identification, ransomware, and foreign or criminal attack
- Independent oversight structure, compelled-access validation and challenge standards, secrecy-order handling, delayed patient notification, public reporting, correction, appeal, sanctions, whistleblower protection, and implementation of the Legislative Requirements Register
- Control separation, independently controlled cryptographic keys, multi-party authorization, immutable external audit, cross-layer access evidence, segmentation, portability, and recovery requirements implementing No Unlogged Access
- Capitalization, protected public funding, service-fee methodology, public-interest subsidies, excess-revenue treatment, acquisition, implementation roadmap, and measurable program milestones

Document Path

Stage	Purpose	Current Status
Concept	Defines mission, value, principles, capabilities, and boundaries.	Version 0.8 prepared for stakeholder review.
Proposal	Defines governance, program case, participation, funding, adoption, and delivery approach.	Pending Concept approval.
Detailed Architecture	Defines implementable technical and operational design.	Pending Proposal approval.
Supporting Documents	Requirements, decisions, security plans, governance policies, roadmaps, and operating procedures.	Developed as the program matures.

Nationwide clinical-prior prefetching, nationwide autorouting capabilities, resistance to abuse and institutional overreach, No Unlogged Access, tripartite policy governance, patient beneficial rights, fiduciary custody, service-cost recovery without data sale, and the Legislative Requirements Register are required NPRR capabilities. The Proposal, legislative program, Detailed Architecture, security plans, governance documents, and operating procedures must preserve these positions and translate them into enforceable and measurable requirements.

Conclusion

NPRR is a proposed national continuity capability built on collaboration, trusted exchange, durable preservation, patient-centered access, and enforceable resistance to misuse. It uses the TEFCA and QHIN foundation, strengthens nationwide identity correlation, supports clinical exchange through FHIR and other approved mechanisms, preserves DICOM as the primary imaging interface, enables authorized nationwide prefetching and controlled autorouting of clinically relevant studies among authorized healthcare organizations, and maintains a high-assurance security posture with independent accountability.

The defining Concept is that a patient's preserved healthcare information should remain available to the patient and appropriately authorized users even when the originating organization cannot respond, while remaining unavailable to actors who lack a specific lawful and authorized purpose. Approval of this Concept establishes the basis for developing the NPRR Proposal.