National Patient Record Repository Concept

Version 0.4

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	0.4
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.

Purpose of This Version

Version 0.4 establishes resistance to abuse, misuse, and institutional overreach as a core NPRR requirement. It defines unacceptable uses, strengthens patient transparency and redress, requires independent oversight, and directs later architecture work to prevent any single institution or administrator from obtaining silent or unilateral access. It retains the national scope, TEFCA alignment, continuity, clinical-prior prefetching, standards positions, security posture, and technology-neutral boundaries established in Version 0.3.

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.

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.

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.

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
- 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, reviewable, and tamper-evident audit records
- 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, or standing administrative path that bypasses normal authorization
- 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, 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.

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.

- 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

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
- Funding, acquisition, contracting, 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.
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.

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.

- National governance, operating authority, stewardship, oversight, and funding
- Participation incentives, onboarding, and phased adoption
- Detailed legal and policy framework for consent, treatment, emergency, disaster, revocation, and secondary use
- NPID issuance, identity proofing, matching, reconciliation, and dispute resolution
- Record retention, correction, provenance, legal hold, archival, and deletion rules
- Nationwide prefetch governance, authorization, relevance algorithms, patient matching, clinical safety, audit, 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, legal process standards, public reporting, patient notification, correction, appeal, sanctions, and whistleblower protection
- Control separation, customer-controlled cryptographic keys, multi-party authorization, tamper-evident external audit, segmentation, portability, and recovery requirements
- Acquisition, cost model, implementation roadmap, and measurable program milestones

Document Path

Stage	Purpose	Current Status
Concept	Defines mission, value, principles, capabilities, and boundaries.	Version 0.4 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 and resistance to abuse, misuse, and institutional overreach are required NPRR capabilities. The Proposal, Detailed Architecture, requirements, governance policies, security plans, operating procedures, and other supporting documents must trace these Concept positions and define how they will be governed, implemented, tested, measured, audited, and enforced.

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 of clinically relevant prior studies, 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.