Open Access Journal on Engineering Applications
ISSN: 3105-7004
www.oajea.hafizlab.com

# EHREP: A Preliminary Design Framework for a FAIR-Compliant Federated Protocol for Electronic Health Record Exchange

**Md Hafizur Rahman**[1,2]

[1]HafizLab
[2]ICT Cell, Jagannath University, Dhaka

**Technical Note Info**
**Received:** 15 April 2026
**Revised:** 25 April 2026
**Accepted:** 01 May 2026
**Published:** 10 May 2026
**Volume No:** 01
**Issue No:** 02
**Page No:** 42-51

**Corresponding author:**
Md Hafizur Rahman
hafizurfpdb@gmail.com

**DOI:**
10.64886/oajea.0102.005v1



**Abstract**

Electronic Health Record (EHR) exchange across heterogeneous healthcare institutions remains a persistent challenge in health informatics and biomedical engineering. Existing solutions — including IHE Cross-Enterprise Document Sharing (XDS), HL7 Direct Protocol, and FHIR Bulk Data API — each address parts of this problem but share a critical limitation: none embeds consent verification and immutable audit trail generation as first-class protocol operations. Furthermore, no globally standardised patient identifier format exists that is simultaneously unique across jurisdictions, privacy-preserving, and deployable in resource-constrained settings. This technical note introduces EHREP (Electronic Health Record Exchange Protocol), a preliminary conceptual framework for a FAIR-compliant, federated, pull-based protocol inspired by the architectural simplicity of the Open Archives Initiative Protocol for Metadata Harvesting (OAI-PMH). EHREP proposes eight protocol verbs, a consent-first data model, a pseudonymisation-by-design identity scheme, a FAIR principle compliance mapping at the protocol specification level, and a novel Global Patient Identifier (EHREP-GPID) format based on country code, identifier type, and hashed national credentials. A cross-border medical tourism scenario — illustrating how a patient treated in Bangladesh can seamlessly share clinical records with a treating physician in Thailand — is presented to demonstrate the practical applicability of the proposed framework. A national-tier extension, the National Health Data Centre (NHDC), is also proposed as a sovereign EHREP harvester node that periodically archives pseudonymised EHR records from domestic hospital nodes and serves as the authoritative cross-border query intermediary for each participating jurisdiction. This work establishes the conceptual foundation and positions EHREP as a novel contribution to the field of interoperable health information exchange, with full protocol specification, implementation, and evaluation planned as future work.

**Keywords:**
Electronic health records, federated protocol, FAIR principles, interoperability, health data exchange, OAI-PMH, consent management, pseudonymisation, global patient identifier, cross-border health data exchange, national health data centre

## 1. Introduction

The widespread adoption of Electronic Health Records (EHRs) has transformed clinical data management across hospitals, clinics, research institutions, and public health agencies [1]. Despite this advancement, patient health data remains predominantly siloed within individual institutions — inaccessible to clinicians at partner facilities, researchers building multi-centre cohorts, or public health authorities monitoring disease outbreaks in real time [2]. The resulting gaps in data continuity lead to duplicate diagnostic procedures, incomplete clinical histories for treating physicians, and delayed responses in public health surveillance.

The consequences of this fragmentation are particularly acute in cross-border healthcare scenarios. Consider a patient who receives diagnostic workup and treatment at a hospital in Dhaka, Bangladesh, and subsequently seeks specialist consultation at a hospital in Bangkok, Thailand. Under current conditions, the Thai physician has no reliable mechanism to access the patient's Bangladeshi clinical records. The patient may carry paper printouts — potentially in Bengali, untranslatable by the receiving system — or may not carry records at all. The result is redundant testing, increased cost, clinical risk from incomplete history, and significant delays in initiating appropriate treatment. This scenario is not hypothetical: Bangladesh is among the countries with the highest rates of outbound medical tourism, with Thailand being a primary destination [20].

**A**chieving true EHR interoperability requires more than data format standardisation. It demands an open, low-barrier exchange protocol that healthcare nodes of any size, vendor ecosystem, or national jurisdiction can implement without prohibitive infrastructure cost [3]. Existing standards — including IHE XDS, HL7 Direct, and FHIR Bulk API — each address parts of this problem but do not embed consent verification or audit trail generation as first-class protocol operations [4]. A further unresolved challenge is the absence of a globally unique, privacy-preserving patient identifier format suitable for cross-institutional and cross-border EHR exchange [16].

**T**his technical note introduces EHREP (Electronic Health Record Exchange Protocol) — a preliminary conceptual framework for a FAIR-compliant [5], federated, pull-based protocol for interoperable EHR exchange across heterogeneous healthcare systems. Drawing on the proven architectural simplicity of OAI-PMH [6], EHREP introduces healthcare-specific protocol primitives — including a consent verification verb, a pseudonymisation-by-design identity model, an immutable audit log verb, a novel Global Patient Identifier format (EHREP-GPID), and a national-tier harvesting architecture (NHDC) — as first-class protocol-level contributions. Full specification, prototype implementation, and evaluation are planned as future work.

## 2. Related Work

### 2.1 EHR Interoperability Standards

Health data interoperability encompasses syntactic, structural, and semantic dimensions [7]. At the syntactic level, HL7 v2 messaging remains deeply embedded in hospital workflows despite well-documented fragmentation. At the structural level, HL7 FHIR R4 has emerged as the dominant modern standard, supported by regulatory mandates including the US 21st Century Cures Act and the European Health Data Space regulation [8]. At the semantic level, controlled vocabularies including SNOMED CT, LOINC, and RxNorm are increasingly mandated to ensure consistent interpretation of exchanged data [9]. Despite this progress, syntactic and semantic interoperability alone do not resolve the exchange problem — healthcare nodes must also agree on how data is requested, authorised, paginated, and audited, which are protocol-layer concerns [10].

### 2.2 Existing Exchange Mechanisms

IHE Cross-Enterprise Document Sharing (XDS) [4] defines a registry-repository model for cross-institutional document exchange. While semantically comprehensive, XDS requires significant infrastructure — Document Source, Repository, Registry, and Consumer actors — making it impractical for resource-constrained institutions. IHE XCA extends XDS for cross-community scenarios but inherits its complexity.

FHIR Bulk Data API [11] provides asynchronous, large-scale FHIR resource export. McMurry et al. [12] demonstrated its effectiveness in the Cumulus federated learning system. However, Bulk FHIR is an API specification, not a protocol: it defines no verb semantics, no resumption-token pagination, and no consent enforcement at the protocol level. HL7 Direct Protocol enables push-based, point-to-point encrypted exchange via secure email but does not support federated pull querying or consent verification [4]. Research into privacy-preserving health data exchange has explored blockchain-based consent management [13] and federated learning frameworks [14], though these do not provide a simple, open, pull-based harvesting protocol.

### 2.3 FAIR Principles in Health Research

The FAIR Guiding Principles — Findable, Accessible, Interoperable, Reusable — were originally proposed for scientific data management [5] and have since been adopted for health research data stewardship [15]. Inau et al. [15] identified a persistent gap: most FAIR initiatives operate at the application or metadata layer rather than at the protocol specification level. EHREP addresses this gap by embedding FAIR compliance into protocol primitives.

### 2.4 OAI-PMH as Architectural Template

OAI-PMH [6], introduced in 2002, demonstrated that a six-verb HTTP pull protocol could achieve global adoption across thousands of repositories. Its stateless HTTP verb invocation, resumption token pagination, selective harvesting by set and datestamp, and simple XML responses provide a proven low-barrier template that EHREP adapts for healthcare.

### 2.5 The Global Patient Identifier Problem

Cross-institutional and cross-border EHR exchange introduces a fundamental identity resolution challenge: a patient known by one identifier at Hospital A may be registered under a different identifier at Hospital B, with no reliable mechanism to determine that both refer to the same individual. The lack of a universal patient identifier results in duplicated medical records and constitutes a serious patient safety issue [16]. Correct patient identification has ranked as the top National Patient Safety Goal published by the Joint Commission for several consecutive years [16].

**E**xisting approaches to cross-domain patient identity resolution include IHE PIXm [17], which provides FHIR-based RESTful transactions for querying a Patient Identifier Cross-reference Manager. However, PIXm is a query and cross-referencing mechanism — it does not define a globally unique, persistent patient identifier format. The United States has no national unique patient identifier standard for health information exchange [18], and no internationally agreed format exists that is simultaneously unique across jurisdictions, privacy-preserving, and deployable in low-resource settings [19]. EHREP addresses this gap with the EHREP-GPID scheme, described in Section 3.3.

### 2.6 Research Gap

No existing published protocol simultaneously satisfies: (1) pull-based federated harvesting paradigm; (2) consent verification as a first-class protocol verb; (3) immutable audit trail generation embedded in the protocol; (4) FAIR compliance at the protocol specification level; (5) low deployment complexity for heterogeneous, resource-constrained systems; (6) a globally unique, privacy-preserving patient identifier scheme operable across jurisdictions; and (7) a national-tier harvesting architecture that consolidates domestic EHR archives while serving as a sovereign cross-border exchange intermediary. EHREP targets this precise intersection.

## 3. EHREP: Conceptual Design Framework

### 3.1 Design Principles

EHREP is grounded in seven core design principles:

- Pull-based sovereignty: Data remains at the source node; requesting nodes pull through protocol verbs with no centralised repository required.
- Consent-first: ConsentVerify is a mandatory protocol step before any data retrieval. Every request must carry a valid, signed ConsentToken.
- Pseudonymisation by design: Patient identifiers are never transmitted in plain form; the protocol returns session-scoped pseudonymous identifiers.
- Audit as a verb: AuditLog is a first-class protocol operation, not a post-hoc logging feature.
- Low barrier: EHREP uses stateless HTTP with JSON/XML responses, requiring no specialised middleware beyond a standard web server.
- Global identity by design: EHREP-GPID provides a jurisdiction-agnostic, privacy-preserving patient identifier scheme as a core protocol element, enabling cross-border patient continuity.
- National-tier archiving: Each country operates a sovereign NHDC that periodically harvests and archives pseudonymised EHR records from domestic nodes, serving as the national EHREP gateway for cross-border exchange.

### 3.2 Protocol Verbs

EHREP defines eight verbs invoked via HTTP GET or POST. Table 1 summarises the proposed verb set. Every request must carry a signed JWT Bearer Token with a purposeOfUse claim (HL7 v3 vocabulary: TREATMENT, RESEARCH, PUBLICHEALTH, PAYMENT).

**E**HREP extends the OAI-PMH error taxonomy with healthcare-specific codes: badArgument, badConsentToken, consentExpired, noRecordsMatch, cannotDisseminateFormat, accessDenied, purposeMismatch, and nodeUnavailable.

Table 1: EHREP Protocol Verbs and Functions

| **Verb** | **HTTP Method** | **Function** |
|---|---|---|
| NodeIdentify | GET | Returns node metadata, FHIR capability statement, and supported clinical formats |
| ListClinicalFormats | GET | Lists supported metadata prefixes (FHIR-R4, CDA, HL7v2) |
| ListPatientSets | GET | Lists available datasets by department, care episode, or clinical condition |
| ConsentVerify | POST | Validates patient consent against FHIR Consent resource; returns signed ConsentToken (JWT) |
| ListPatientIdentifiers | GET | Returns pseudonymised EHREP-GPID list with resumptionToken for pagination |
| HarvestRecords | GET | Batch pull of consented EHR records in NDJSON, cryptographically signed |
| GetClinicalRecord | GET | Retrieves single EHR record by EHREP-GPID; triggers AuditLog automatically |
| AuditLog | POST | Writes immutable access event to both nodes; returns AuditAck confirmation |

### 3.3 EHREP-GPID: Proposed Global Patient Identifier Format

A core contribution of EHREP is the proposal of a structured, globally unique, privacy-preserving patient identifier — EHREP-GPID — as a first-class protocol element. EHREP-GPID bridges the gap identified in Section 2.5 by providing a jurisdiction-agnostic identifier scheme operable across heterogeneous national identity systems.
The EHREP-GPID follows a four-component structure:

```
EHREP-GPID ::= [CountryCode]-[IDTypeCode]-[HashedCredential]-[CheckDigit]
```

where CountryCode is the ISO 3166-1 alpha-2 two-letter country code; IDTypeCode is a standardised code identifying the type of national credential used; HashedCredential is the HMAC-SHA256 hash of the raw national credential, keyed with the issuing node's secret key; and CheckDigit is a single verification digit (algorithm deferred to the full EHREP specification as future work). Representative examples:

```
BD-NID-a3f9c2d1e4b5f6a7b8c9d0e1f2a3b4c5d6e7f8a9-4   (Bangladesh, National ID)
GB-NHS-b2e8d1c3f4a5b6c7d8e9f0a1b2c3d4e5f6a7b8c9-7   (United Kingdom, NHS Number)
SG-NRC-c1d2e3f4a5b6c7d8e9f0a1b2c3d4e5f6a7b8c9d0-2   (Singapore, NRIC)
US-MRH-d0e1f2a3b4c5d6e7f8a9b0c1d2e3f4a5b6c7d8e9-9   (USA, Hashed MRN fallback)
```

Table 2: EHREP-GPID proposed ID Type Codes and fallback hierarchy

| **Code** | **Meaning** | **Example Countries** | **Priority** |
|---|---|---|---|
| NID | National Identity Card Number | Bangladesh, India, Malaysia, Egypt | 1 (highest) |
| NHS | National Health Service Number | United Kingdom, Commonwealth nations | 1 |
| NRC | National Registration / NRIC | Singapore, Brunei | 1 |
| BRN | Birth Registration Number | Countries without universal NID | 2 |
| PPN | Passport Number (cross-border fallback) | Any jurisdiction | 3 |
| MRH | Hashed Medical Record Number (local) | Any institution without national ID | 4 (lowest) |

The fallback hierarchy (Table 2) ensures that EHREP-GPID can be generated for any patient in any country, regardless of whether a national identity scheme exists. In all cases, the raw credential is hashed before inclusion — never stored or transmitted in plain form. EHREP-GPID is natively compatible with the HL7 FHIR Patient resource identifier field using the system URI urn:ehrep:gpid.

### 3.4 Illustrative Use Case: Cross-Border Patient Continuity (Bangladesh to Thailand)

To ground the EHREP design in a concrete real-world scenario, this section presents an illustrative use case involving a patient who receives clinical care in Bangladesh and subsequently seeks specialist consultation in Thailand. This scenario is representative of a growing class of cross-border medical tourism cases in which the absence of an interoperable exchange protocol results in clinical risk, redundant testing, and treatment delays [20].

*Scenario (Table 3): A patient in Dhaka, Bangladesh, undergoes diagnostic investigation — including blood panels, imaging, and a biopsy — at a tertiary hospital. The results indicate a condition requiring specialist management. The patient travels to Bangkok, Thailand, for specialist consultation. The Thai physician requires the full clinical history, laboratory results, imaging metadata, and biopsy report to initiate appropriate treatment without redundant investigation.*

Under current conditions, no protocol exists by which the Thai physician can securely and automatically retrieve the patient's Bangladeshi clinical records with verified consent and an immutable access audit. EHREP addresses this scenario through the following protocol exchange sequence:

Table 3: EHREP cross-border exchange sequence — Bangladesh to Thailand.

| Step | EHREP Verb / Action | Description |
|---|---|---|
| 1 | Patient consent (BD) | Before departure, the patient provides explicit digital consent at the Bangladeshi hospital node. The FHIR Consent resource is created with purpose of Use: TREATMENT, scoped to the Thai hospital node. |
| 2 | EHREP-GPID generation (BD) | The Bangladeshi node generates the patient's EHREP-GPID: BD-NID-[hash]-4. A PPN fallback is also generated: BD-PPN-[hash]-6. The patient receives this as a QR code or secure mobile token. |
| 3 | NodeIdentify (TH → BD) | The Thai hospital node invokes NodeIdentify against the Bangladeshi node to confirm EHREP capability, supported clinical formats, and FHIR R4 compatibility. |
| 4 | ConsentVerify (TH → BD) | The Thai node submits the patient's EHREP-GPID and ConsentToken. The Bangladeshi node validates the FHIR Consent resource and returns a signed JWT ConsentToken confirming authorised TREATMENT access. |
| 5 | HarvestRecords (TH → BD) | Using the ConsentToken, the Thai node invokes HarvestRecords with metadataPrefix: FHIR-R4. The Bangladeshi node returns the complete clinical records as a signed NDJSON FHIR Bundle. |
| 6 | Semantic resolution | The Thai system automatically interprets FHIR R4 records using SNOMED CT and LOINC codes. No manual translation or format conversion is required, regardless of original documentation language. |
| 7 | AuditLog (TH + BD) | An immutable AuditLog entry is written to both nodes, recording the access event, timestamp, EHREP-GPID, and ConsentToken reference. Both institutions retain a tamper-evident audit record. |

This exchange sequence demonstrates how EHREP's eight protocol verbs operate in concert to enable secure, consent-gated, audited cross-border EHR exchange. The patient's raw National ID is never transmitted; the Thai physician gains full clinical access within a single protocol exchange; both institutions retain an immutable audit trail; and FHIR R4 with SNOMED CT and LOINC ensures semantic interpretability without manual translation. In an NHDC-enabled deployment, Steps 3–5 would be mediated through the Bangladesh NHDC rather than directly to the hospital node, further simplifying node discovery and reducing direct cross-border query load on individual hospitals.

### 3.5 FAIR Principle Compliance Mapping

A core contribution of EHREP is operationalising the FAIR principles at the protocol specification level rather than the application layer [15]. Table 4 maps each FAIR criterion to a specific EHREP mechanism.

Table 4: FAIR principle compliance mapping in EHREP.

| Principle | Criterion | EHREP Mechanism |
|---|---|---|
| Findable | Persistent identifier | Each node and dataset assigned a DOI/UUID; NodeIdentify exposes DCAT-AP descriptors; EHREP-GPID provides persistent cross-border patient-level identifier; NHDC maintains national dataset catalogue. |
| Findable | Rich metadata | ListClinicalFormats and ListPatientSets return DCAT-AP compliant metadata; NHDC exposes national-level DCAT-AP dataset descriptors. |
| Accessible | Open protocol | HTTPS standard; NodeIdentify and NHDC discovery endpoint publicly accessible without authentication. |
| Accessible | Authentication | OAuth 2.0 + JWT Bearer Token; X.509 mutual TLS for node and NHDC channels; ConsentToken for patient-level access. |
| Interoperable | Standard vocabulary | metadataPrefix enforces FHIR-R4 / CDA / HL7v2; terms resolved via SNOMED CT, LOINC [9]; cross-border semantic transparency via NHDC. |
| Interoperable | Qualified references | HarvestRecords responses include provenance links to source node DOI and version; NHDC maintains provenance chain. |
| Reusable | Licence metadata | Every response includes ODRL licence field (CC BY 4.0 or proprietary); NHDC enforces national data licence policy. |
| Reusable | Provenance | AuditLog generates immutable FHIR AuditEvent chain traceable to ConsentToken; NHDC retains national audit archive. |

### 3.6 Security Model Overview

EHREP adopts a zero-trust security posture. All node-to-node and node-to-NHDC communication is secured via TLS 1.3 with X.509 mutual certificate authentication. Application-level authorisation uses attribute-based access control (ABAC) evaluated against the requesting node's JWT claims, the declared purposeOfUse, and the data subject's current FHIR Consent resource status. Patient identifiers are pseudonymised using a session-scoped HMAC-SHA256 scheme. EHREP-GPID credentials are hashed at the point of identifier generation and never stored or transmitted in plain form. In cross-border scenarios, the ConsentToken issued by the source node is time-limited and purpose-scoped. The NHDC operates as a trusted national gateway, maintaining its own X.509 certificate issued under a nationally governed Public Key Infrastructure (PKI), ensuring that cross-border NHDC-to-NHDC channels are independently verifiable by both participating jurisdictions.

## 4. Comparison with Existing Protocols

Table 5 provides a qualitative comparison of EHREP against the three most relevant existing exchange mechanisms across seven dimensions, including the cross-border patient continuity and national-tier archiving capabilities introduced by EHREP.

As Table 5 illustrates, EHREP is the only proposed mechanism in which consent verification, audit trail generation, a globally unique privacy-preserving patient identifier, cross-border patient continuity, and a national-tier EHR archive architecture are all first-class protocol-level contributions, and in which FAIR compliance is designed into the protocol specification rather than delegated to application-layer implementations.

## 5. Discussion

The EHREP framework is deliberately preliminary. Several design decisions remain open for subsequent work: the formal ConsentToken schema and its relationship to FHIR Consent resource versions; the precise pseudonymisation cryptographic properties under re-identification attack models; the resumptionToken expiry

Table 5: Qualitative comparison of EHREP with existing EHR exchange protocols.

| **Dimension** | **IHE XDS** | **FHIR Bulk API** | **Direct Protocol** | **EHREP (proposed)** |
|---|---|---|---|---|
| Paradigm | Push/Registry | Pull (API) | Push (email) | Pull (protocol) |
| Consent as verb | No | No | No | Yes |
| Audit as verb | No (ATNA) | No | No | Yes |
| FAIR compliance | Partial | Partial | No | Full (by design) |
| Global patient ID | No | No | No | Yes (EHREP-GPID) |
| Cross-border continuity | Partial | No | No | Yes (by design) |
| National archive (NHDC) | No | No | No | Yes (proposed) |
| Deployment complexity | High | Medium | Medium | Low (target) |

and error recovery semantics for large batch harvests; the governance model for multi-jurisdictional node federation; and the formal check digit algorithm and collision resistance analysis for EHREP-GPID.

**T**he NHDC proposal introduces additional open challenges that require careful future analysis. The harvesting schedule and retention policy of the NHDC — how frequently domestic nodes are harvested, what data granularity is archived, and how long records are retained — will significantly affect both the utility and the privacy risk profile of the national archive. The NHDC must also operate under a nationally governed data protection framework (e.g., the Personal Data Protection Act in Bangladesh or Singapore, or GDPR-equivalent legislation), and bilateral trust agreements between NHDCs of different countries must be established before cross-border NHDC-to-NHDC queries can be authorised. These governance and legal dimensions are as important as the technical design and will be addressed in a dedicated future research contribution.

**A**key adoption challenge for EHREP will be the transition from existing infrastructure. Institutions running IHE XDS or FHIR endpoints should be able to expose an EHREP interface as a thin protocol adapter layer without replacing underlying data stores. The OAI-PMH precedent is instructive: global adoption was achieved because any web server returning XML could become a compliant node. EHREP targets the same low-barrier philosophy for healthcare [3], recognising that cross-border interoperability at scale requires protocols that smaller institutions in any jurisdiction can implement.

## 6. Future Work

This technical note establishes the conceptual foundation for EHREP. The following activities are planned as part of a doctoral research programme:

- Full formal specification of EHREP verbs, request/response schemas, and error taxonomy, formatted as an RFC-style technical standard.
- Formal specification of the EHREP-GPID check digit algorithm, collision analysis, and re-identification attack resistance properties under adversarial models.
- Formal security model under a zero-trust network assumption, including threat modelling and cryptographic analysis of the pseudonymisation and GPID hashing schemes.
- Open-source reference implementation in Python (FastAPI) with an EHREP Conformance Test Suite, including a simulated cross-border exchange scenario between two EHREP nodes.
- Quantitative comparative evaluation of EHREP against IHE XDS, FHIR Bulk API, and Direct Protocol across deployment complexity, protocol latency, consent overhead, FAIR compliance coverage, and cross-border patient identity resolution accuracy.
- Governance framework for multi-jurisdictional EHREP federation, addressing bilateral and multilateral trust agreement models for cross-border NHDC-to-NHDC deployment.

### 6.1 National Health Data Centre (NHDC) — Proposed Architecture

A national-tier extension of EHREP is envisioned in which each participating country operates a National Health Data Centre (NHDC) — a sovereign EHREP harvester node that periodically harvests pseudonymised EHR archives from domestic hospital nodes and serves as the authoritative cross-border query intermediary for that jurisdiction. The proposed two-tier EHREP harvesting model operates as follows:

- Tier 1 — Domestic harvesting: The NHDC periodically invokes HarvestRecords against all registered domestic hospital and clinic EHREP nodes on a configurable schedule (e.g., nightly or weekly). Harvested records are stored in pseudonymised FHIR R4 NDJSON format, indexed by EHREP-GPID. Raw patient identifiers are never stored at the NHDC level.
- Tier 2 — Cross-border intermediation: When a foreign EHREP node or NHDC requests a patient's records, the request is routed through the patient's home-country NHDC. The NHDC performs ConsentVerify against the domestic consent registry, and if authorised, serves the archived FHIR Bundle — eliminating the need for the foreign node to directly query individual domestic hospital nodes.
- NHDC-to-NHDC trust: Cross-border NHDC-to-NHDC channels are secured by X.509 certificates issued under a nationally governed PKI, with bilateral trust agreements defining permissible purposeOfUse values, data retention limits, and audit obligations.
- Fallback mode: In jurisdictions where an NHDC has not yet been established, EHREP continues to operate in direct node-to-node mode — preserving backward compatibility and ensuring that NHDC deployment is an optional enhancement rather than a prerequisite.

The NHDC architecture (Figure 1) is depicted conceptually below. Full formal specification of the NHDC — including its harvesting schedule policy, data retention framework, national PKI integration, bilateral trust agreement model, and disaster recovery design — is planned as a dedicated research contribution within the EHREP doctoral programme.

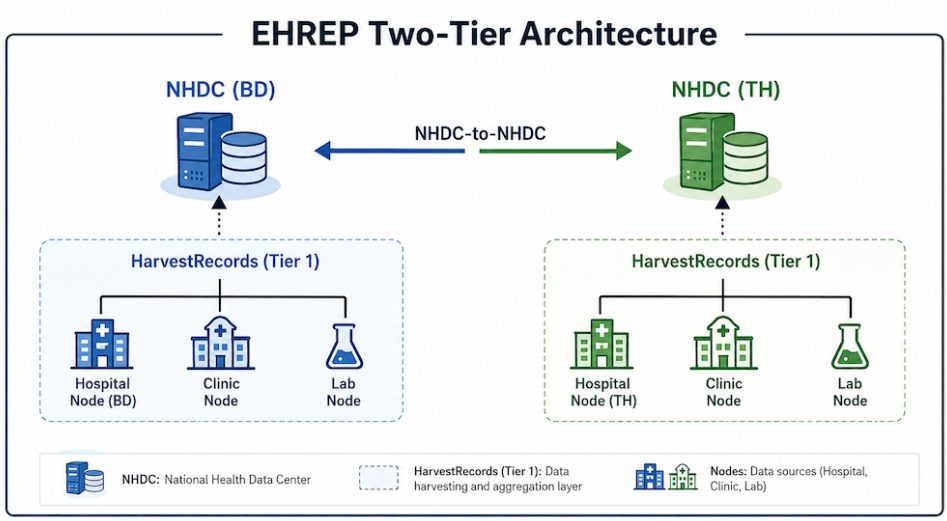


Figure 1: EHREP Two-Tier Architecture

## 7. Conclusion

This technical note has introduced EHREP, a preliminary conceptual framework for a FAIR-compliant, federated, pull-based protocol for interoperable EHR exchange across heterogeneous healthcare systems. Drawing on the architectural simplicity of OAI-PMH, EHREP proposes eight protocol verbs — including ConsentVerify and AuditLog as first-class operations — a consent-first data model, a full FAIR compliance mapping at the protocol specification level, a novel EHREP-GPID format for globally unique privacy-preserving patient identification, a cross-border use case demonstrating how a patient treated in Bangladesh can seamlessly share clinical records with a treating physician in Thailand, and a proposed National Health Data Centre (NHDC) architecture as a sovereign two-tier EHR harvesting and cross-border intermediation layer. A qualitative comparison with existing mechanisms demonstrates that EHREP occupies a novel position in the design space: no existing published

protocol simultaneously achieves pull-based federation, protocol-embedded consent verification, immutable audit logging, FAIR compliance, a jurisdiction-agnostic patient identifier scheme, cross-border patient continuity, and a national-tier EHR archive architecture. Future work will develop EHREP from this conceptual foundation into a formally specified, implemented, and evaluated open standard for health data exchange.

## 8. Declarations

Conflict of Interest: The author declares that this research was conducted without any commercial or financial relationships constituting a potential conflict of interest. The author is an editor of OAJEA; this submission was handled by an independent editor in accordance with COPE guidelines.

**F**unding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

**A**uthor Contributions: Md Hafizur Rahman: Conceptualisation, methodology, writing — original draft, writing — review and editing.

**T**he author used Claude (Anthropic) as an AI writing assistant for drafting and iterative refinement of this manuscript. All intellectual contributions, conceptual framework design, and final editorial decisions are the sole responsibility of the author.

**D**ata Availability: No datasets were generated or analysed. This is a conceptual/design paper.

**E**thical Approval: Not applicable. This study does not involve human participants, human data, or animal subjects.

## References

[1] J. R. Vest and L. D. Gamm, "Health information exchange: persistent challenges and new strategies," Journal of the American Medical Informatics Association, vol. 17, no. 3, pp. 288–294, 2010. https://doi.org/10.1136/jamia.2010.003673.

[2] E. P. Kansiime, J. M. Ondulo, and C. O. Odoyo, "Navigating the interoperability landscape of electronic medical record systems in developing countries: a narrative literature review," Journal of Science, Innovation and Creativity, vol. 3, no. 2, pp. 18–34, 2024. https://doi.org/10.58721/jsic.v3i2.733.

[3] E. T. Inau, J. Sack, D. Waltemath, and A. A. Zeleke, "Initiatives, concepts, and implementation practices of FAIR data principles in health data stewardship: scoping review," Journal of Medical Internet Research, vol. 25, p. e45013, 2023. https://doi.org/10.2196/45013.

[4] IHE International, "IHE IT Infrastructure Technical Framework: Cross-Enterprise Document Sharing (XDS.b)," Rev. 20.0, IHE International, 2023. [Online]. Available: https://www.ihe.net/resources/technical_frameworks

[5] M. D. Wilkinson et al., "The FAIR Guiding Principles for scientific data management and stewardship," Scientific Data, vol. 3, p. 160018, 2016. https://doi.org/10.1038/sdata.2016.18.

[6] C. Lagoze and H. Van de Sompel, "The Open Archives Initiative: Building a low-barrier interoperability framework," in Proc. ACM/IEEE Joint Conf. Digital Libraries (JCDL), Portland, OR, USA, 2002, pp. 54–62. https://doi.org/10.1145/379437.379449

[7] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design science in information systems research," MIS Quarterly, vol. 28, no. 1, pp. 75–105, 2004. https://doi.org/10.2307/25148625.

[8] European Commission, European Health Data Space (EHDS) Regulation, Official Journal of the European Union, 2024. [Online]. Available: https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_en

[9] A. Chatterjee, N. Pahari, and A. Prinz, "HL7 FHIR with SNOMED-CT to achieve semantic and structural interoperability in personal health data: a proof-of-concept study," Sensors, vol. 22, no. 10, p. 3756, 2022. https://doi.org/10.3390/s22103756

[10] O. A. Adepoju, O. T. Yusuf, and B. A. Ogunboye, "A critical review of health data interoperability standards: FHIR, HL7, and beyond," ResearchGate Preprint, 2025. https://www.researchgate.net/publication/392786216_A_Critical_Review_of_Health_Data_Interoperability_Standards_FHIR_HL7_and_Beyond

[11] HL7 International, "SMART/HL7 Bulk FHIR Access Implementation Guide," Release 2.0, HL7 International, 2023. [Online]. Available: https://hl7.org/fhir/uv/bulkdata

[12] A. J. McMurry et al., "Cumulus: A federated EHR-based learning system powered by FHIR and AI," medRxiv, Feb. 2024. https://doi.org/10.1101/2024.02.02.24301940.

[13] R. Walambe, V. Potdar, and K. Kotecha, "A systematic review of privacy-preserving methods deployed with blockchain and federated learning for telemedicine," Healthcare Analytics, vol. 3, p. 100192, 2023. https://doi.org/10.1016/j.health.2023.100192.

[14] S. Lee, Y. Kim, and S. Cho, "Searchable blockchain-based healthcare information exchange system to enhance privacy preserving and data usability," Sensors, vol. 24, no. 5, p. 1582, 2024. https://doi.org/10.3390/s24051582

[15] A. Kiourtis et al., "Electronic health records at people's hands across Europe: the InteropEHRate protocols," in Proc. 19th Int. Conf. Wearable Micro Nano Technologies Personalized Health (pHealth), Oslo, Norway, 2022, pp. 145–150. https://doi.org/10.3233/SHTI220973

[16] HIPAA Journal, "Time to stop blocking a national patient identifier system," HIPAA Journal, Aug. 2025. [Online]. Available: https://www.hipaajournal.com/time-to-stop-blocking-a-national-patient-identifier-system

[17] IHE IT Infrastructure Technical Committee, "Patient Identifier Cross-referencing for Mobile (PIXm)," Release 3.1.0, IHE International, 2023. [Online]. Available: https://profiles.ihe.net/ITI/PIXm

[18] M. A. Ward, P. Russo, and J. R. Ferris, "Universal patient identifier and interoperability for detection of serious drug interactions: retrospective study," JMIR Medical Informatics, vol. 8, no. 12, p. e23539, 2020. https://doi.org/10.2196/23353

[19] WHO and UNAIDS, "Considerations and guidance for countries adopting national health identifiers," UNAIDS Guidance Document JC2640E, Geneva, Switzerland, 2014. [Online]. Available: https://www.unaids.org/sites/default/files/media_asset/JC2640_nationalhealthidentifiers_en.pdf

[20] Razwan Ahamed , Cross-Border Medical Tourism in South Asia: Legal, Ethical, and Policy Dimensions of Bangladeshi Patient Mobility, 9 (1) IJLMH Page 1806 - 1814 (2026). https://doi.org/10.10000/IJLMH.1111374