

Security-Aware and Privacy-Preserving Personal Health Record Sharing using Consortium Blockchain

Prof. Ramachandra H Y

Assistant Professor,
Dept. of CSE
Shridevi Institute of Engineering
and Technology, Tumkur, India

Arpita Kodihalli

Dept. of CSE
SIET, Tumkur, India

Divya K B

Dept. of CSE
SIET, Tumkur, India

Noorain Afsha

Dept. of CSE
SIET, Tumkur, India

Abstract - Sharing a patient's clinical history across independent hospitals is often hindered by fragmented record-keeping, centralized databases that create single points of failure, and the absence of a mechanism that keeps the patient in control of who may view their data. This paper presents an implemented prototype of a security-aware and privacy-preserving Personal Health Record (PHR) sharing system built around a consortium blockchain of participating hospitals. A patient registers once at an originating hospital and receives a system-generated unique patient identifier that is bound to a registered mobile number. When the same patient visits a second, independent hospital, the receiving hospital requests the identifier and the system issues a one-time password (OTP) to the patient's registered mobile number; the record is released only after the correct OTP is supplied, so possession of the identifier alone never grants access. Every registration, record-creation, and cross-hospital access event is written to an append-only access-log ledger maintained by the consortium, giving hospitals and patients a traceable audit trail. A working web-based prototype implementing patient registration, hospital-side record creation, OTP-gated cross-hospital retrieval, and a log dashboard was developed; representative screenshots of each module are analyzed. The results indicate that patient-initiated, OTP-bound authorization combined with a permissioned blockchain audit layer can give patients practical, demonstrable control over cross-hospital sharing of their health information.

Keywords - *consortium blockchain; personal health record; one-time password; patient-centric access control; healthcare data privacy; audit trail.*

I. INTRODUCTION

Healthcare organizations routinely generate large volumes of sensitive patient information, including diagnoses, prescriptions, laboratory findings, and treatment histories. When a patient moves between hospitals — for a referral, a

second opinion, or an emergency admission — timely access to prior records can materially improve clinical decision-making. In practice, however, most hospitals maintain this information in isolated, centrally administered databases. Such databases are convenient for a single institution but poorly suited to inter-hospital sharing: they concentrate trust in one operator, offer limited transparency into who accessed a record and when, and give the patient little practical say over onward disclosure of their own data.

Blockchain technology has been widely discussed as a way to address these shortcomings because a distributed ledger can make record-access events tamper-evident and independently verifiable by every participant, without relying on a single centralized administrator. For a healthcare setting, a permissioned or consortium blockchain — in which only vetted hospitals, clinics, and allied institutions may operate a node — is generally preferred over a fully public ledger, since participants must be accountable, credentialed organizations rather than anonymous parties.

Most existing blockchain-based health-record proposals concentrate on ledger design, consensus, and cryptographic access-control policies, and comparatively few describe a simple, end-to-end authorization step that an ordinary hospital reception or records desk can carry out without specialized blockchain tooling. This paper addresses that practical gap by describing an implemented prototype in which authorization to view a record hinges on two factors held jointly by the patient: the unique patient identifier issued at registration and a one-time password delivered to the patient's registered mobile number at the moment a second hospital requests access. Neither factor alone is sufficient, and the whole exchange is recorded on a consortium ledger for later audit.

The contributions of this work are summarized as follows:

- A patient-centric, two-factor cross-hospital authorization workflow — unique patient ID plus registered-mobile OTP — that does not require the

requesting hospital to already hold any part of the patient's record.

- A consortium blockchain layer that records registration, record-creation, and access events as an append-only, auditable log rather than storing raw clinical text on-chain.
- A working web-based prototype covering patient registration, first-hospital record creation, second-hospital OTP-gated retrieval, and an access-log dashboard, evaluated here through representative captured screenshots of each module.

II. RELATED WORK

Several early efforts explored blockchain as a substrate for medical-record management. Azaria et al. proposed MedRec, a decentralized framework in which smart contracts encode a patient's ownership of, and permissions over, records that continue to reside in providers' own databases; the blockchain itself stores only pointers and permission metadata rather than clinical content [1]. Xia et al. presented MeDShare, aimed specifically at trust-less sharing of medical data among cloud service providers, using smart contracts and an on-chain provenance trail to track how a data set moves between organizations and to detect misuse after the fact [2].

Zhang et al. introduced FHIRChain, which combines blockchain with the HL7 FHIR clinical-data standard to make shared records more interoperable across differing hospital information systems, while still keeping bulk data off-chain [3].

Dagher et al. proposed Ancile, a framework that layers proxy re-encryption and fine-grained, attribute-based access-control policies over an Ethereum-style ledger so that a patient can revoke or scope a provider's access after it has been granted [4]. More broadly, Christidis and Devetsikiotis surveyed how blockchains and self-executing smart contracts can automate multi-party workflows in the Internet-of-Things and adjacent domains, providing much of the conceptual basis later applied to healthcare [5], and Engelhardt discussed the practical opportunities and obstacles of introducing blockchain into hospital IT environments [6].

Taken together, this body of work establishes that a distributed ledger can provide tamper-evident provenance, fine-grained permissioning, and cross-institution trust for health data. However, these designs are largely oriented toward smart-contract-level access-control policy and cryptographic key management, which presumes staff and patients who are comfortable operating blockchain wallets or attribute-based encryption keys. Comparatively little attention has been paid to a lightweight, front-desk-operable authorization step — of the kind already familiar from banking and e-commerce one-time-password flows — that a patient can invoke unassisted at a second hospital using only an identifier and their own phone. The prototype described in this paper targets that specific, practical gap: it keeps the ledger's role focused on immutable event logging while placing the moment-of-access authorization decision in the patient's hands through an OTP challenge.

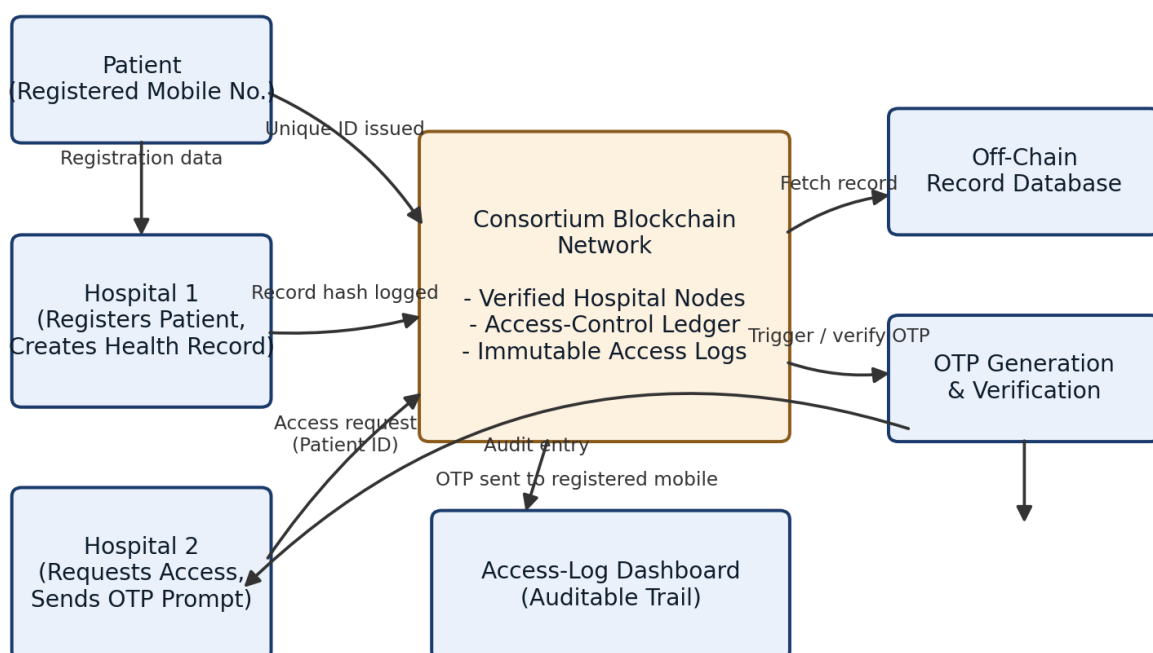


Fig. 1. Architecture of the proposed consortium-blockchain PHR sharing system.

III. PROPOSED SYSTEM ARCHITECTURE

Fig. 1 summarizes the architecture of the proposed system. Four categories of participant interact through a consortium blockchain network: the patient, the originating hospital that first registers the patient and creates a record, any subsequent hospital that later requests access, and the consortium ledger itself, which is jointly maintained by the verified hospital nodes.

Only credentialed hospitals may operate a node in the consortium, which distinguishes this design from a public, permissionless chain and keeps the set of parties who can propose or validate an access event limited to accountable healthcare organizations. Rather than writing full clinical text on-chain, and consistent with earlier designs that keep bulk clinical data off the ledger and record only pointers or provenance metadata on it [1], [2], the ledger here is used to record registration events, a reference to each newly created health record, and every subsequent access attempt together with its outcome; the clinical content itself is kept in an off-chain record database associated with the originating hospital, in the same spirit as the off-chain data handling used in FHIRChain [3]. This separation keeps the ledger small and fast to replicate while still giving every consortium member a verifiable history of who touched a given patient's record and when.

A. Patient Identity and Registration

When a patient first registers, the system binds the patient's name, registered mobile number, and email to a freshly generated unique patient identifier. This identifier is the only credential the patient needs to carry between hospitals; it is deliberately insufficient on its own to retrieve any record.

B. OTP-Gated Cross-Hospital Access

When a second hospital enters a patient identifier to request a record, the system generates a one-time password and delivers it to the mobile number bound to that identifier at registration. The requesting hospital can proceed only once the patient supplies the correct, time-bound OTP, which the second hospital then submits back to the system for verification before the record is released. This single-use, time-limited credential design follows established authentication guidance for one-time secrets [7], and gives the patient an explicit, revocable say over each disclosure in the same way that attribute-based, patient-revocable permissions do in Ancile [4], but through a simpler mechanism that does not require the patient to manage cryptographic keys.

C. Consortium Ledger and Audit Trail

Each registration, record-creation, and access event — successful or otherwise — is appended to an access-log ledger shared across consortium nodes. Because entries are append-only, a hospital cannot quietly erase evidence of a past access, and a patient or auditor can later reconstruct a complete history

of which hospitals viewed a given record and under what circumstance.

IV. IMPLEMENTATION AND SYSTEM MODULES

The prototype was implemented as a web application exposing a small set of role-specific pages: a landing dashboard, a patient-registration form, a first-hospital record-creation form, a second-hospital lookup-and-OTP flow, and an access-log dashboard. The following subsections walk through each module together with representative captured screens of the running system.

A. Landing Dashboard

Fig. 2 shows the application's home page, titled “Secure Personal Health Record System – Consortium Blockchain Healthcare Application”, which exposes four entry points corresponding to the four core modules: patient registration, hospital-side record access, health-record creation, and the access-log viewer.



Fig. 2. Landing dashboard of the PHR sharing application.

B. Patient Registration

A new patient supplies their name, mobile number, and email through the registration form shown in Fig. 3. On submission, the system confirms the registration and returns a system-generated unique patient identifier (Fig. 4), which the patient is instructed to retain for use at any other consortium hospital.

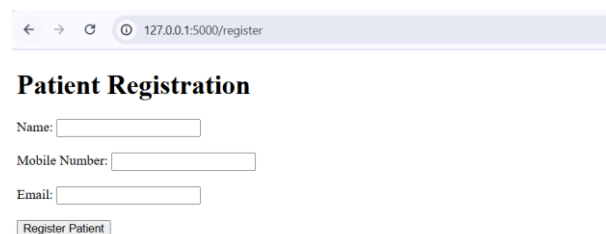


Fig. 3. Patient registration form.

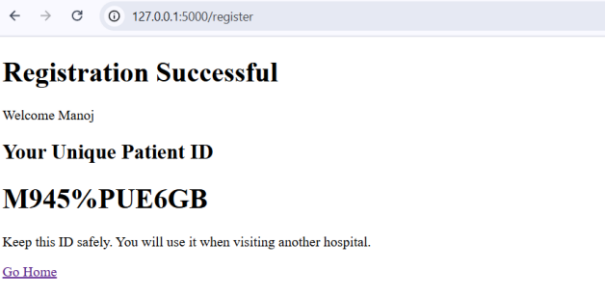


Fig. 4. Registration confirmation showing the system-generated unique patient identifier.

C. Health Record Creation at the Originating Hospital

Fig. 5 shows the record-creation form used by the originating hospital. Hospital staff enter the patient's unique identifier together with the hospital name, diagnosis, and treatment details, after which the record is stored and referenced from the consortium ledger.

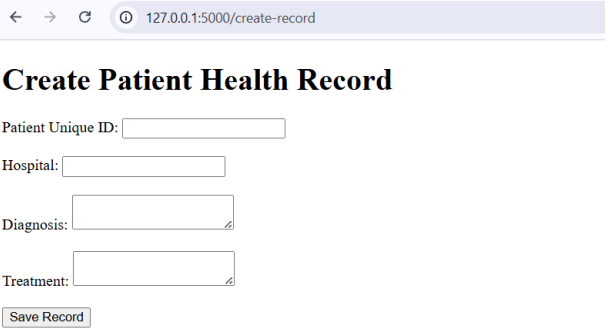


Fig. 5. Health-record creation form used by the originating hospital.

D. Cross-Hospital OTP-Gated Retrieval

At a second, independent hospital, staff enter only the patient's unique identifier to look up the record (Fig. 6). The system does not display any clinical information at this stage; instead, it triggers an OTP challenge (Fig. 7), and the receiving hospital must submit the six-digit code obtained from the patient before the authorized record view (Fig. 8) — including patient name, identifier, and associated medical records — is released.

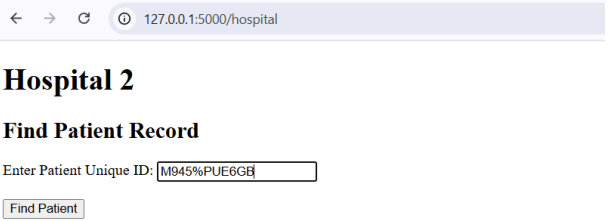


Fig. 6. Second hospital looking up a patient record by unique identifier.

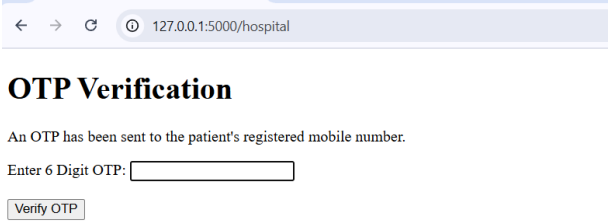


Fig. 7. OTP verification prompt issued before record release.



Fig. 8. Authorized patient record view after successful OTP verification.

E. Access-Log Dashboard

Fig. 9 shows the access-log dashboard, which lists every recorded access event together with the patient identifier, the requesting hospital, the action performed, and a timestamp. In the captured demonstration, the log shows a series of OTP-authorized accesses by “Hospital 2” against several distinct patient identifiers, illustrating the kind of audit trail the consortium ledger is intended to preserve.

Patient ID	Hospital	Action	Date
M945%PUE6GB	Hospital 2	Patient record accessed using OTP	2026-09-11 11:27:19.248075
T397V0#64B%	Hospital 2	Patient record accessed using OTP	2026-09-01 19:35:22.877812
NB6T05A@NTE	Hospital 2	Patient record accessed using OTP	2026-09-01 19:19:07.398124
ZOZDLDEA05G	Hospital 2	Patient record accessed using OTP	2026-09-01 19:16:53.209551
FS0W0ILN8SC	Hospital 2	Patient record accessed using OTP	2026-09-01 19:14:25.736940
A105FVK8BCS	Hospital 2	Patient record accessed using OTP	2026-09-01 19:12:00.349730
ZIPK8X8G80J	Hospital 2	Patient record accessed using OTP	2026-09-01 19:08:13.251962
SJXORX05QO#	Hospital 2	Patient record accessed using OTP	2026-09-01 19:04:57.681559
LR0P7@QHFVC	Hospital 2	Patient record accessed using OTP	2026-09-01 19:00:52.112387
MPFPL5YARUS	Hospital 2	Patient record accessed using OTP	2026-09-01 18:55:54.861889
JS38%80QU59	Hospital 2	Patient record accessed using OTP	2026-09-01 18:53:35.336028
T397V0#64B%	Hospital 2	Patient record accessed using OTP	2026-09-01 18:43:49.080223

Fig. 9. Access-log dashboard showing the auditable trail of OTP-authorized accesses.

V. SECURITY AND PRIVACY ANALYSIS

The design separates two things that are often conflated in simpler systems: knowing a patient's identifier and being authorized to view that patient's record. Table I summarizes the principal threats considered during the design of the prototype and the corresponding mitigation built into the workflow.

TABLE I. THREATS CONSIDERED AND CORRESPONDING MITIGATIONS

Threat / Risk	Mitigation in the Prototype
Identifier alone used to impersonate a patient at another hospital	Record release additionally requires a time-bound OTP sent to the registered mobile number; the identifier alone is non-functional
Undetected or repudiated access by a hospital	Every access attempt is appended to a shared, append-only consortium ledger visible to all member nodes
Single point of failure / unilateral tampering by one hospital	Ledger state is replicated across verified hospital nodes rather than held by a single administrator, following the distributed-trust rationale used in MeDShare [2]
Exposure of clinical text to parties who only need to verify identity	Off-chain record database stores clinical content separately from the ledger, which records references and events rather than raw diagnoses
OTP interception or reuse	OTP is single-use and time-bound; production deployment should add attempt-rate limiting, discussed in Section VII

Because the second hospital never learns the record contents until the patient actively cooperates by relaying the OTP, a lost or guessed identifier cannot by itself be used to pull a patient's history. This is a deliberate trade-off: it adds one interactive step to every cross-hospital lookup in exchange for keeping the patient in the authorization loop at the exact moment their data is requested.

VI. RESULTS AND DISCUSSION

The captured demonstration registers a patient, “Manoj,” who receives the identifier M945%PUE6GB (Fig. 4). A subsequent lookup of this identifier at Hospital 2 (Fig. 6) triggers the OTP challenge in Fig. 7; once verified, the authorized view in Fig. 8 confirms the patient's name and identifier, though in the captured run no prior diagnosis had yet been attached to that particular identifier, which the interface correctly reports as “No medical records found” rather than failing or exposing an error.

The access-log dashboard (Fig. 9) independently corroborates this flow: it lists the M945%PUE6GB lookup alongside eleven other OTP-authorized accesses by Hospital 2 against distinct identifiers, each with its own timestamp. This is the behavior expected of an audit-oriented ledger — every access attempt, not only successful clinical retrievals, becomes part of the permanent record available to any consortium participant.

Overall, the demonstration supports the central design claim: the two-factor combination of identifier and OTP is sufficient to gate cross-hospital retrieval in ordinary operation, and the resulting log gives a simple, human-readable audit trail without

requiring hospital staff to interact with blockchain primitives directly.

VII. LIMITATIONS

Several limitations of the current prototype should be acknowledged. First, the demonstrated system runs as a single local web service (127.0.0.1:5000); the consortium ledger's multi-node replication and consensus behavior have not been exercised across physically separate hospital nodes. Second, OTP delivery is described conceptually as an SMS-based channel bound to the registered mobile number, but the captured screenshots do not evidence an integration with a live telecom or SMS gateway, so delivery latency and failure handling remain untested. Third, no throughput, latency, or scalability measurements were collected for the ledger under concurrent access from multiple hospitals. Fourth, the interface does not yet visibly enforce OTP attempt limits or lockout after repeated failures, which a production deployment would require. Finally, encryption of the off-chain clinical database at rest and in transit is assumed but not directly observable from the available screenshots, and a formal security proof of the authorization protocol has not been carried out.

VIII. FUTURE WORK

Planned extensions include deploying the ledger on a genuine permissioned blockchain runtime with multiple independent hospital nodes to validate consensus and replication under realistic network conditions; integrating a live SMS or push-notification gateway for OTP delivery with configurable expiry and attempt-rate limiting; adding fine-grained, attribute-based access control so that individual clinicians, rather than a hospital as a whole, can be scoped to specific record types and have that access revoked afterward; encrypting off-chain clinical data at rest with per-record keys; and conducting a formal threat-model evaluation and load testing across a larger, multi-hospital consortium before any production use.

IX. CONCLUSION

This paper described an implemented prototype of a security-aware, privacy-preserving personal health record sharing system that combines a consortium blockchain audit layer with a patient-held, two-factor authorization step consisting of a unique identifier and a registered-mobile OTP. Captured screenshots of patient registration, record creation, OTP-gated cross-hospital retrieval, and an access-log dashboard demonstrate that the workflow functions end-to-end and produces a traceable audit history of every access attempt. While the current prototype has not yet been evaluated at multi-node, production scale, the results suggest that keeping the patient actively in the loop at the moment of cross-hospital access — rather than relying solely on cryptographic policy enforced invisibly on-chain — is a practical and understandable way to give patients real control over who sees their health information.

ACKNOWLEDGMENT

The authors acknowledge the guidance of Prof. Ramachandra H Y, Assistant Professor, Department of Computer Science and Engineering, and thank Shridevi Institute of Engineering and Technology, Tumkur, for the support provided throughout the development of this project.

REFERENCES

- [1] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using Blockchain for Medical Data Access and Permission Management," in Proc. 2nd Int. Conf. Open and Big Data (OBD), 2016, pp. 25–30.
- [2] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain," IEEE Access, vol. 5, pp. 14757–14767, 2017.
- [3] P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosenbloom, "FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data," Computational and Structural Biotechnology Journal, vol. 16, pp. 267–278, 2018.
- [4] G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, "Ancile: Privacy-Preserving Framework for Access Control and Interoperability of Electronic Health Records Using Blockchain Technology," Sustainable Cities and Society, vol. 39, pp. 283–297, 2018.
- [5] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," IEEE Access, vol. 4, pp. 2292–2303, 2016.
- [6] M. A. Engelhardt, "Hitching Healthcare to the Chain: An Introduction to Blockchain Technology in the Healthcare Sector," Technology Innovation Management Review, vol. 7, no. 10, pp. 22–34, 2017.
- [7] National Institute of Standards and Technology, "Digital Identity Guidelines: Authentication and Lifecycle Management," NIST Special Publication 800-63B, 2017.