Balancing Patient Privacy and Health Data Security: The Role of Compliance in Protected Health Information (PHI) Sharing

Md Al Amin[a], Hemanth Tummala[b], Rushabh Shah[c] and Indrajit Ray[d]
Computer Science Department, Colorado State University, Fort Collins, Colorado, U.S.A.

Keywords: Consent, Patient Privacy, Data Security, PHI Sharing, Provenance, Compliance, Blockchain, Smart Contract.

Abstract: Protected Health Information (PHI) sharing significantly enhances patient care quality and coordination, contributing to more accurate diagnoses, efficient treatment plans, and a comprehensive understanding of patient history. Compliance with strict privacy and security policies, such as those required by laws like HIPAA, is critical to protect PHI. Blockchain technology, which offers a decentralized and tamper-evident ledger system, hold promise in policy compliance. This system ensures the authenticity and integrity of PHI while facilitating patient consent management. In this work, we propose a blockchain technology that integrates smart contracts to partially automate consent-related processes and ensuring that PHI access and sharing follow patient preferences and legal requirements.

1 INTRODUCTION

Acquiring patient consent for healthcare information sharing is paramount for adhering to policy compliance, particularly concerning regulations like the Health Insurance Portability and Accountability Act (HIPAA) in the U.S. and the General Data Protection Regulation (GDPR) in the E.U (Hutchings et al., 2021). These regulatory frameworks emphasize protecting health information and upholding the patient's right to privacy. Patient consent is a cornerstone of these regulations, ensuring individuals have control over their health data and its dissemination. Under HIPAA, healthcare entities must obtain explicit consent before sharing healthcare data for purposes beyond treatment, payment, or healthcare operations. Similarly, GDPR enforces strict guidelines on data consent, processing, and privacy, offering individuals the 'right to be forgotten' and the autonomy to decide how their data is used and shared. From a policy compliance perspective, proper patient consent acquisition is a legal requirement and a trust-building measure, reinforcing the patient-provider relationship. It ensures transparency in data handling and builds patient confidence, knowing their sensitive information is shared respectfully and responsibly. As healthcare continues to integrate with various technologies, upholding these consent protocols is crucial for maintaining the security and privacy of patient data and adhering to global data protection standards.

Unauthorized health data access and disclosure are common events in healthcare industries that increase security and privacy concerns. Table 1 shows the number of compliance complaints received by the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) (Rights (OCR), 2008). The primary reasons for the complaints are (i) impermissible uses and disclosures of PHI, (ii) lack of safeguards of PHI, (iii) lack of patient access to their PHI, (iv) lack of administrative safeguards of electronic PHI, and (v) use or disclosure of more than the minimum necessary PHI. These issues can be minimized by enforcing patients' consent for data access and sharing decisions and employing proper data protection mechanisms like encryption and anonymity. Consent lets patients control their healthcare journey, enabling them to make choices that align with their best interests and well-being (Timmermans, 2020).

Enhanced security and privacy technologies are essential for protecting patient data from being compromised, misused, or disclosed. However, substantial evidence indicates that the root of many unauthorized EHR access and sharing lies in inadequate policy adoption, implementation, and enforcement (Lopez Martinez et al., 2023; Aljabri et al., 2022). Often, users are granted access privileges inappropri-

[a] https://orcid.org/0000-0003-1700-7201
[b] https://orcid.org/0009-0007-7778-5845
[c] https://orcid.org/0009-0005-5658-0950
[d] https://orcid.org/0000-0002-3612-7738

Al Amin, M., Tummala, H., Shah, R. and Ray, I.
Balancing Patient Privacy and Health Data Security: The Role of Compliance in Protected Health Information (PHI) Sharing.
DOI: 10.5220/0012767400003767

In *Proceedings of the 21st International Conference on Security and Cryptography (SECRYPT 2024)*, pages 211-223
ISBN: 978-989-758-709-2; ISSN: 2184-7711

Table 1: OCR HHS- Compliance Complaints.

Year	Complains	Compliance Reviews	Technical Assistance	Total
2018	25089	438	7243	32770
2019	29853	338	9060	39251
2020	26530	566	5193	32289
2021	26420	573	4244	31237

ately, whether intentionally or not. Policy compliance frequently falls short, and access control measures are not rigorously monitored or executed on time. A common oversight is the blanket assignment of identical roles and privileges to all employees, neglecting the nuances of individual patient-level policies. Moreover, auditing and monitoring practices are typically reactive, triggered only by serious complaints or legal mandates, rather than proactive and consistent. These policy specification and enforcement flaws significantly impact informed consent policies, underscoring the need for a more accurate and systematic approach to effectively protecting patient healthcare data and preserving privacy.

It is essential to address the following concerns to guarantee compliance with the applicable privacy and security policies, industry best practices, and contractual obligations for sharing PHI: (i) Patient-level policies or consents are often not properly or timely enforced in healthcare data sharing. (ii) Patients lack assurance that consent for access or sharing purposes is carried out strictly by designated users, and only if the stipulated conditions are met are all other requests rejected. (iii) Data sharing over email or other mediums is insecure due to the absence of encryption or the use of inadequate and weak encryption algorithms and key sizes. (iv) The centralized hospital system serves as a singular source of truth and a potential single point of failure for managing audit trails. (v) The absence of a verifiable, unaltered record for consent execution and sharing PHI highlights the need for comprehensive consent provenance. (vi) Compliance assessments and audits are not conducted accurately and timely to check compliance status.

To address the aforementioned challenges and requirements, this paper proposes a framework based on blockchain and smart contracts for managing and enforcing informed consent when sharing PHI with entities outside the treatment team. The approach ensures that PHI sharing occurs only when the sender has obtained the necessary consent from the patient and the sharing aligns with specific, predefined purposes. In addition to enforcing patient consent, this approach integrates other relevant security policies and industry best practices to ensure data protection. The HIPAA Security Rule mandates the requirements for transmission security are outlined under 45 CFR § 164.312(e)(1) Technical Safeguards (Chung et al., 2006). However, the proposed approach does not directly guarantee security mechanisms like encryption for data protection. Instead, it leverages an honest broker who acts as a blind and secure entity to evaluate the intended PHI and certify its status as required protection mechanisms are satisfied or not (Alarcon et al., 2021) . The broker's attestation is then recorded in blockchain-based audit trails with other relevant activity data to support future compliance evaluations and validation. It supports using audit trails or provenance mechanisms based on blockchain, which is essential for keeping track of PHI-sharing activities. Moreover, the proposed framework provides a compliance-checking mechanism in data-sharing activities, ensuring adherence to applicable policies.

Smart contracts, (Buterin et al., 2014), offer an automated, transparent system that upholds the integrity and accountability of the consent for sharing PHI. Through this smart contract-based approach, the proposed framework not only automates processes but also guarantees the accurate execution of informed consent, thereby enhancing the security and reliability of PHI sharing. Blockchain technology ensures the immutability of submitted records, safeguarding the integrity of the audit trail and enabling the detection of any unauthorized alterations. Blockchain security features, including non-repudiation, ensure that participants cannot deny their actions (Le and Hsu, 2021).

This work is the first to capture patients' informed consent for PHI sharing to ensure policy compliance through preserving provenance and conducting compliance checking. It also considers and enforces other applicable security policies and industry best practices mandated by the various laws, regulations, standards, and contractual obligations to meet the compliance requirements. Significant contributions include (i) implementing a mechanism to capture patients' consent for sharing healthcare data beyond the treatment team members. (ii) Storing obtained consents in decentralized and distributed networks (blockchain) to overcome a single point of truth sources and failure. (iii) Considering applicable security and privacy policies, regulatory requirements, and contractual obligations to ensure compliance-based sharing. (iv) Enforcing informed consent and applicable policies while making authorization decisions to share health records. (v) Equipping blockchain-based audit trail mechanisms to guarantee data provenance. (vi) Incorporating compliance assessment methods to identify compliance and non-compliance PHI sharing. (vii) Offering consent services to provide precise and comprehensive insights into the consent granted and the extent of its execution.

2 RELATED WORK

Blockchain technology has increasingly been adopted in healthcare for various services, particularly for sharing protected health information among healthcare providers, patients, and other stakeholders. Blockchain facilitates a more efficient, transparent, and patient-centered delivery of healthcare services, making it an essential component in modern healthcare infrastructure. Fan et al., (Fan et al., 2018), proposed a blockchain-based secure system, MedBlock, to share electronic medical records among authorized users. It provides security and privacy with access control protocols and encryption technology while sharing patient healthcare data.

Shah et al., (Shah et al., 2019), proposed a medical data management framework to facilitate data sharing. It gives patients full control over access to their medical data. It also ensures that patients know who can access their data and how it is used. Zhuang et al., (Zhuang et al., 2020), addressed a blockchain-based patient-centric health information-sharing mechanism protecting data security and privacy, ensuring data provenance, and providing patients full control over their health data. However, consent structure and compliance requirements are not addressed, which are very important to give patients confidence in how their consent is executed and how data is protected.

Alhajri et al., (Alhajri et al., 2022), explored the criticality of implementing legal frameworks to safeguard privacy within fitness apps. By examining how various fitness apps handle consent and privacy policies, their research highlighted the crucial role of consent as outlined in the GDPR. The authors proposed the adoption of blockchain technology as a means to govern user consent for sharing, collecting, and processing fitness data, ensuring a process centered around human needs and compliant with legal standards. Nonetheless, the study failed to present a technical architecture for their blockchain-based proposal.

Amofa et al. approached a blockchain-based personal health data sharing framework with an underlying mechanism to monitor and enforce acceptable use policies attached to patient data (Amofa et al., 2018). Generated policies are consulted with smart contracts to make decisions on when the intended data can be shared or otherwise. All entities cooperate to protect patient health records from unauthorized access and computations. Balistri et al., (Balistri et al., 2021), designed the *BlockHealth* solution for sharing health data with tamper-proofing and protection guarantees. They store the patient's healthcare data in a private database, and the hash of the healthcare data is stored in the blockchain to ensure data integrity.

The above-mentioned papers summarized the application and benefits of using blockchain for healthcare data sharing and essential services. However, they failed to address the security and privacy requirements mandated by various laws and regulatory agencies, such as HIPAA and GDPR. The major requirements demand patient consent and proper protection, such as encryption, while sharing health records. In addition, it is crucial to maintain audit logs and check that those activities did not violate any policies. This paper proposes sharing informed consent as the smart contract for authorization with provenance and compliance-checking mechanisms.

3 PROPOSED APPROACH

The main objective is to ensure compliance with applicable security and privacy policy for PHI sharing. To ensure compliance, we need proper policy enforcement, including maintaining provenance and performing compliance status checks promptly and properly. For enforcement, this paper considers patient-informed consent, where the sender has permission from the patient to share the intended PHI with the receiver for specific purposes. Also, proper data protection mechanisms are considered. However, instead of ensuring data protection directly, this work leverages an honest broker to verify and certify the data protection mechanism. PHI-sharing activities are recorded as audit trails to provide provenance and reconstruct events in a manner that reflects their actual occurrence. A private blockchain-based approach is proposed (Section 4). Finally, a blockchain consensus mechanism called Proof of Compliance (PoC) is approached, Section 5, for performing auditing. This audit rigorously examines the enforcement actions against the policy standards and informed consent, using the provenance data to verify and certify the policy's compliance status while sharing health records. The seamless connection between policy enforcement, provenance, and the auditing process forms the backbone of a secure and compliant system.

3.1 Patient-Provider Agreement (PPA)

The patient-provider agreement, or PPA, aims to determine who is responsible for what in treatment. A PPA is formed when a patient visits a hospital and is properly documented to deliver healthcare services. It differs from organization to organization. Healthcare organizations adjust what they need from patients and what they expect from them to match those needs,

treatments, and responsibilities. This is done based on the nature and needs of treatment and services. Also, the components and representation of the PPA depend on the hospital or clinic. Figure 1 shows the structure of a PPA, and Algorithm 1 illustrates the gradual processes for creating a PPA with the required components. The main concept of PPA is adopted from (Al Amin et al., 2023). The authors focused on consent management for medical treatment and diagnosis purposes, mainly for the treatment team members. They did not include patient consent and other requirements for health data sharing beyond the treatment team. This paper extends the PPA structure to analyze the requirements and formalize the consent components for PHI sharing. A PPA is formally composed of five tuples:

$$PPA = (PC, PrC, TIC, SIC, ROC)$$

satisfying the following requirements:

(A) *PC* is a finite set of patient components containing the patient's personal information, contact information, mailing information, pharmacy information, billing and insurance information, emergency contact, and others. The patient is responsible for providing and maintaining these components' valid, accurate, and updated information.

(B) *PrC* is a finite set of provider components, including the treatment team, prescription, and others. The provider is responsible for creating an effective team to provide appropriate care. Everything from treatment to insurance coverage and billing is considered during the patient treatment period.

(C) *TIC* is a finite set of treatment informed consent components. It denotes that the patient has permitted the designated treatment team to access medical records. Treatment team members include doctors, nurses, support staff, lab technicians, billing officers, emergency contact persons, and others assigned by the authority. Some outsider members are insurance agents, pharmacists/pharmacy technicians, doctors/lab technicians from another hospital, etc.

(D) *SIC* is a finite set of sharing informed consent components. It denotes the patient's consent to sharing medical data for a specific purpose. Both the sender and the receiver must have consent. The primary purpose of this work is *SIC*, including (i) identifying, capturing, and storing consent components, (ii) enforcing consents with other applicable security policies and industry best practices to ensure policy compliance while making PHI-sharing decisions, (iii) defining and capturing provenance information with the enforced consents to maintain audit trails, (iv) performing compliance checking using consensus mechanisms; (v) providing services for both given and executed consents, etc. It does not consider other components: *PC*, *PrC*, *TIC*, and *ROC*.

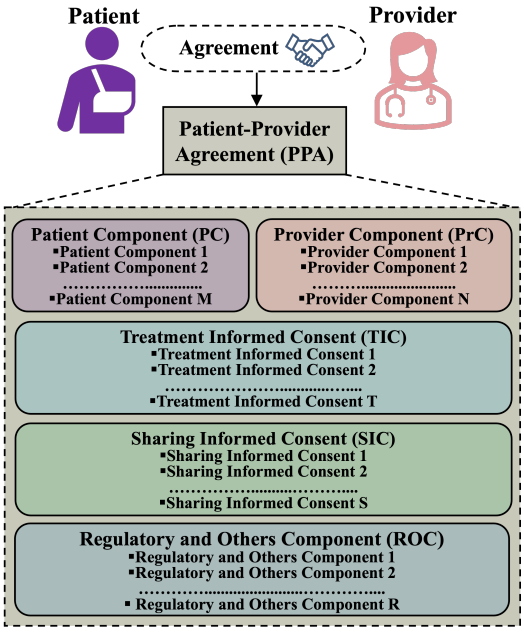

Figure 1: Patient-Provider Agreement (PPA) Components.

(E) *ROC* is a finite set of regulatory and other components. It has applicable security and privacy policies to comply with the requirements of local government, state government, federal government, foreign government, and regulatory agencies (HIPAA, GDPR) if necessary. It also includes contractual obligations in some cases.

3.2 Sharing Informed Consent (SIC)

Before approving, patients need to know clearly about the sharing informed consent, particularly who can share which PHI with whom for what purposes—and also the protection mechanism while sharing PHI during transmission over the network. Figure 2 shows the SIC conceptual framework structure. Sharing informed consent is formally composed of four tuples:

$$SIC = (S, R, PHI, P)$$

satisfying the following requirements:

(a) S is a finite set of authorized senders denoted as $\{S_1, S_2, S_3, ...S_s\}$ for s number of senders. The sender can share certain healthcare data with the receiver, who has permission from the patient. The sender may be a member of the patient treatment team or anyone from the provider.

Algorithm 1: Patient-Provider Agreement (PPA) Formation.

Input : (i) PC, (ii) PrC, (iii) TIC, (iv) SIC, (v) ROC, (vi) $\mathbb{R}_{PPA}$, (vii) $\mathbb{BN}_{SC}$

/* $\mathbb{R}_{PPA}$: secured PPA repository, BN_{SC}: blockchain network smart contract */

Result: A formal PPA

Input Parameters Initialization

$PPA_i \leftarrow \{PC_i, PrC_i, TIC_i, SIC_i, ROC_i\}$ where i is patient identity

(i) $PC \leftarrow \{PC_1, PC_2, PC_3, PC_4, PC_5, PC_6 ..... PC_M\}$

(ii) $PrC \leftarrow \{PrC_1, PrC_2, PrC_3, PrC_4, PrC_5, PrC_6 ..... PrC_N\}$

(iii) $TIC \leftarrow \{TIC_1, TIC_2, TIC_3, TIC_4, TIC_5, TIC_6 ..... TIC_T\}$

(iv) $SIC \leftarrow \{SIC_1, SIC_2, SIC_3, SIC_4, SIC_5, SIC_6 ..... SIC_S\}$

(v) $ROC \leftarrow \{ROC_1, ROC_2, ROC_3, ROC_4, ROC_5, ROC_6 ... ROC_R\}$

PPA Components Integrity Calculation /* $\mathbb{H}(\partial)$ calculates hash of ∂ */

(a) $\mathbb{H}_{PC} \leftarrow \mathbb{H}(PC_1, PC_2, PC_3, PC_4, PC_5, PC_6 ..... PC_M)$

(b) $\mathbb{H}_{PrC} \leftarrow \mathbb{H}(PrC_1, PrC_2, PrC_3, PrC_4, PrC_5, PrC_6 ..... PrC_N)$

(c) $\mathbb{H}_{TIC} \leftarrow \mathbb{H}(TIC_1, TIC_2, TIC_3, TIC_4, TIC_5, TIC_6 ..... TIC_T)$

(d) $\mathbb{H}_{SIC} \leftarrow \mathbb{H}(SIC_1, SIC_2, SIC_3, SIC_4, SIC_5, SIC_6 ..... SIC_S)$

(e) $\mathbb{H}_{ROC} \leftarrow \mathbb{H}(ROC_1, ROC_2, ROC_3, ROC_4, ROC_5, ROC_6 .. ROC_R)$

(f) $\mathbb{H}_{PPA_i} \leftarrow \mathbb{H}(\mathbb{H}_{PC}, \mathbb{H}_{PrC}, \mathbb{H}_{TIC}, \mathbb{H}_{SIC}, \mathbb{H}_{ROC})$

PPA Finalization if PPA_i *is complete* **then**

/* presence of PC, PrC, TIC, SIC, ROC */

if $(\mathbb{R}_{PPA} + PPA_i)$ *contains no conflicts* **then**

(i) do $\mathbb{R}_{PPA} \leftarrow (\mathbb{R}_{PPA} + PPA_i)$

(ii) add $\mathbb{ID}_{PPA_i}$ to patient profile, $\mathbb{P}_i$

(iii) call $\mathbb{BN}_{SC}(\mathbb{ID}_{PPA_i}, \mathbb{H}_{PPA_i})$

/* PPA integrity verification reference */

Return: Success (PPA_i added to $\mathbb{R}_{PPA}$)

else

Error: $(\mathbb{R}_{PPA} + PPA_i)$ contains conflicts

/* PPA_i revision required to add */

end if

else

Error: PPA_i cannot be created (incomplete PPA)

end if

(b) R is a finite set of authorized users who receive protected health information from authorized senders. A finite set of r number authorized receivers denoted as $\{R_1, R_2, R_3, ...R_r\}$. The receiver may be from other hospitals, labs, medical research institutes, pharmaceutical companies, marketing departments, government officials, etc.

(c) PHI is a finite set, d number, of health data denoted by $\{PHI_1, PHI_2, PHI_3, ...PHI_d\}$. It is an electronic version of a patient's medical data that healthcare providers keep over time. They are protected health information and contain sensitive patient information. PHI must be protected from any kind of unauthorized access, disclosure, and sharing. Table 2 shows ten (10) types of PHI, considered for each patient, with PHI ID, name, description, and potential creators.

(d) P is a finite set of purposes. It indicates the objective of the PHI sharing by the senders with the receivers. Receivers must use the received PHI for the intended purposes. A finite set of purposes, a

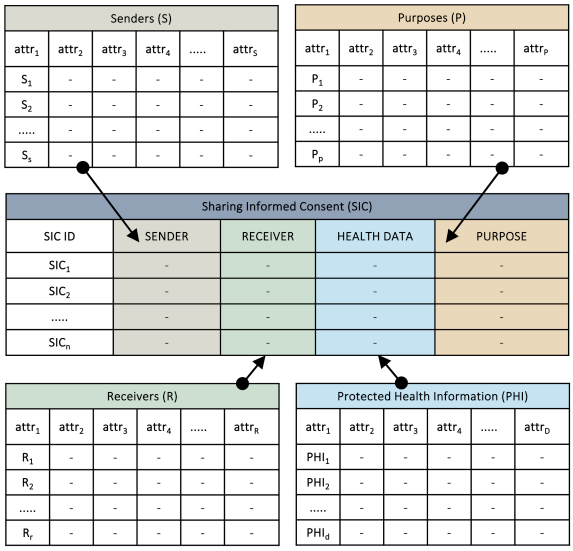

Figure 2: Sharing Informed Consent (SIC) Structure.

p number, can be denoted as $\{P_1, P_2, P_3, ...P_p\}$.

The objective of sharing protected health information outlines the specific reasons for its sharing. The recipient must utilize the shared PHI exclusively for its designated purpose. The potential reasons for sharing PHI in this study include, but are not limited to:

(i) ***Treatment:*** Providers or patients need to share PHI with other providers from external hospitals to provide better treatment. Also, patients must move to different regions, like states or countries, due to family movement, job transfers, or new jobs. Patients need to share or transfer healthcare data from the previous providers to the current.

(ii) ***Diagnosis:*** Present providers sometimes need more skilled human resources, appropriate machinery, instruments, or sophisticated technology to diagnose disease. But it is urgently required to do that to give proper treatment and services to save patients' lives or minimize damages. Patients' health data must be transferred or shared with other providers or labs to complete diagnosis and make proper treatment plans for the patients.

(iii) ***Marketing:*** Healthcare data sharing for marketing purposes involves using patient data to promote healthcare services, products, or initiatives. This can help healthcare providers tailor their services to patient needs, inform patients about new treatments or products, and improve patient engagement. Only the receiver entity can use the shared data as intended and should not share it with other associates for extended business purposes.

(iv) ***Research:*** Sharing PHI for medical research purposes holds significant potential for advancing

Table 2: Sample Patient Protected Health Information (PHI) Structure.

PHI ID	PHI Name	PHI Description	PHI Creator
PHI-1001	Demographic Information	Basic personal information like name, date of birth, gender, contact	Patient, Support Staff
PHI-1002	Previous Medical History	Old medical records from another hospitals and providers	Patient, Support Staff
PHI-1003	Immunizations, Vaccinations	Immunization records that are administered over time	Patient, Pathology Lab Technician
PHI-1004	Allergies	Various allergies sources, triggering condition, remediation	Patient, Support Staff, Path Lab Tech
PHI-1005	Visit Notes	Physiological data, advises, follow-up, visit details	Doctor, Nurse
PHI-1006	Medications, Prescription	Pharmacy information, prescribed medications like name, dosage	Doctor
PHI-1007	Pathology Lab Works	Biological samples analysis like blood, tissue, other substances	Pathology Lab Technician
PHI-1008	Radiology Lab Works	Imaging results such as X-rays, CT, MRI, Ultrasound, PET scans	Radiology Lab Technician
PHI-1009	Billing, Insurance	Bank account, credit/debit card, and insurance policy information	Patient, Support Staff, Billing Officer
PHI-1010	Payer Transactions	Bills of doctor visit, lab works, and medications	Billing Officers, Insurance Agent

medical knowledge, leading to breakthroughs in understanding diseases, improving and developing new treatments, improving healthcare systems and services, and enhancing patient outcomes. Patients' privacy and rights must be respected.

Other purposes might exist depending on the nature and requirements of the treatment, patient conditions, provider business policy, etc. This study considers only the four purposes mentioned above. After receiving shared data, the receiver performs specified operations to complete the job. It is assumed that the receiver cannot share data with other users who do not have permission from the patients. More specifically, the receiver's healthcare system does not allow the sharing of PHI by any means, like printouts, email, or screenshots. However, this paper doesn't provide detailed mechanisms or techniques for preventing data sharing without patients' consent at the receiver end.

3.3 SIC Smart Contract Deployment

Once a Patient-Provider Agreement, or PPA, is created and stored in the repository, all sharing informed consent components are deployed to the blockchain network. For each patient, there is one smart contract that contains all consents for that particular patient. If there isn't a smart contract, the authority deploys one, transfers ownership to the patient, and updates the contract address to the patient's profile and hospital systems. The contract address is an identifier for a smart contract in the blockchain network. This smart contract-based approach provides an automated system and guarantees the integrity and accountability of the deployed consents. Once consents are deployed or added to the smart contract, they cannot be altered. The authorization module needs to access these smart contracts to make decisions considering the sender, receiver, purpose attributes, environmental factors, organizational policies, regulatory frameworks, etc.

Upon finalizing the PPA, it transforms and secures storage in a PPA repository. Subsequently, an integrity marker, such as a hash ($\mathbb{H}_{PPA_i}$) generated by

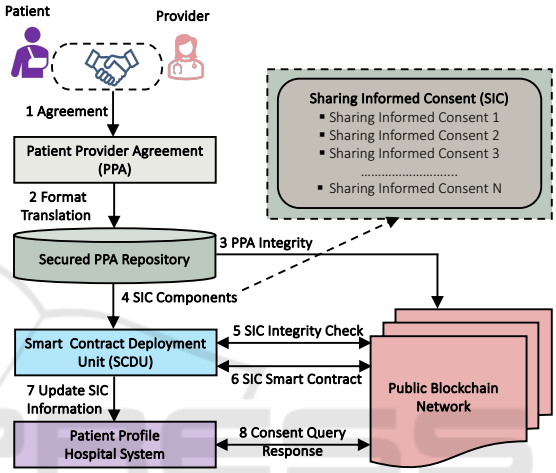

Figure 3: SIC Smart Contract Deployment Process.

the Algorithm 1, is stored on the blockchain alongside the PPA ID for later modification detection. These are depicted in Steps 2 and 3 in Figure 3. The Smart Contract Deployment Unit (SCDU) then gathers all components of the informed consent from the PPA (Step 4). It verifies their integrity to ensure no deliberate or accidental alterations have occurred (Step 5). As a secure entity, the SCDU does not alter consent components, noting that any modification invalidates the consent. If the consents remain unmodified, the SCDU creates and deploys the corresponding smart contracts on the blockchain network (Step 6) and then updates the patient's profile and the hospital system (Step 7). Users can make queries with the required credentials regarding informed consent and get responses in Step 8 from the blockchain network.

3.4 Honest Broker, Applicable Policies and Industry Best Practices

Alongside patient consent, the proposed approach incorporates relevant security policies and industry best practices before sharing protected health information. For instance, a security policy might require a data

protection mechanism during data transfer between systems. For treatment and diagnosis purposes, encryption is a recommended protection method.

Similarly, anonymity is a recommended protection method for marketing and research purposes, where patient identifiers must be removed before sharing. The targeted PHI must be anonymous using proper techniques and tools before sending the data from the host healthcare system to the receiver. The host system indicates where patients' PHI is created or presently stored. Healthcare organizations deploy appropriate encryption and anonymity mechanisms. This study does not directly ensure PHI encryption and anonymity. Instead, this approach leverages an honest broker, a trusted entity that evaluates the encryption algorithm, key size, and data anonymity status (Alarcon et al., 2021). After checking, the honest broker certifies or attests to the status, which is recorded in audit trails as proof for policy compliance verification, along with other components like sharing informed consents, timestamps, etc.

3.5 PHI Sharing Authorization Process

Consent enforcement ensures that related consents are executed while making decisions for the PHI sharing requests. All consents are stored on the public blockchain network as smart contracts and cannot be enforced until they are called. The authorization module (AM) considers sharing informed consent with applicable policy and required attributes while making decisions. The attributes may be subject, object, operation, and environmental attributes. The sender must provide the necessary credentials for identification and authentication. Figure 4 shows the informed consent enforcement for PHI-sharing authorization.

A sender submits a data sharing request to the PHI sharing unit in *Step 1*. Sharing unit forwards request to authorization module for decision in *Step 2*. It also requests that the PHI storage unit send the intended PHI to the protection mechanism unit in *Steps 2a* and *2b*. The honest broker receives encrypted or anonymized data in *Step 3*. After analyzing, it sends a report to AM in *Step 4*. The AM queries the blockchain network through the corresponding smart contract to get sharing informed consent information for the sharing request in *Step 3a* and *4a*. It also makes queries for requests related to applicable policies and required attributes in *Steps 3b* and *3c*. It receives the policy and attributes in *Steps 4b* and *4c*. After evaluating, it makes an authorization decision and sends it to the sharing unit in *Step 5*. If the request is approved, the sharing unit gets encrypted or anonymized data based on the purpose in *Steps 7a* and *7b*. Then, it delivers the intended PHI through email or protocol to the receiver in *Step 8*.

The audit trail recording unit collects logs from AM in *Step 6a* and from the honest broker in *Step 6b*. It combines logs and stores as an audit trail in *Step 6c* in Private Audit Blockchain. Section 4 discusses block structure and others. The compliance status checking is done in *Steps 9a, 9b*, and *9c* by the Proof of Compliance consensus mechanism. Compliance status reports are produced in *Step 10*. Section 5 discusses the required mechanism. For this study, it is considered that the authorization module is not compromised or tampered with. It is the reference monitor for making access decisions and must be tamper-proof (Mulamba and Ray, 2017). Also, the communication channel between AU and the smart contract access points or apps is secured from malicious users.

4 PHI SHARING PROVENANCE

Enforcing an applicable set of policies is crucial, but preserving data provenance to show adherence to these policies is also essential. Nevertheless, policy compliance cannot be quantified or confirmed in isolation. An independent auditor conducts a thorough policy audit to verify compliance with the policy, utilizing the available provenance data to ascertain and certify the policy's compliance status. For an accurate policy compliance assessment, two critical elements must be diligently maintained: *(i) consent and policy lineage* and *(ii) PHI sharing activity audit trails*. This section contains the detailed provenance mechanisms dedicated to preserving the policy lineage's integrity and ensuring the audit trails' authenticity.

4.1 Consent and Policy Lineage

Policy lineage involves a comprehensive record of all policies that guide the authorization module's decisions. It's a transparent and traceable record of the policy history and its application in decision-making processes. For this study, sharing informed consent is mainly considered for decision-making. Since all consents are deployed as smart contracts, blockchain networks can create policy lineages. However, this paper does not consider other HIPAA-related policies, such as physical security, provider training, etc (Chung et al., 2006).

4.2 PHI Sharing Activity Audit Trails

Integrity in policy enforcement ensures that events are documented faithfully, reflecting the sequence and na-

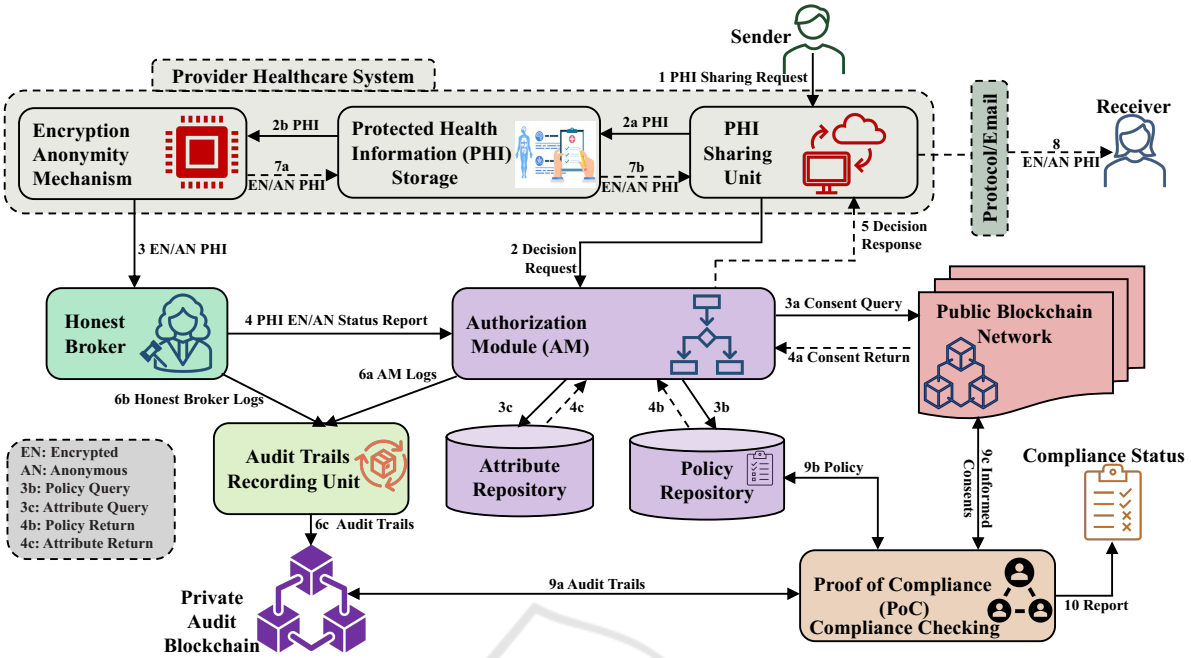

Figure 4: Compliance-based PHI Sharing Authorization Process.

ture of actions taken. This authenticity is crucial for transparency and accountability. Provenance plays a key role by offering a detailed and unalterable history of policy enforcement actions as they are carried out, safeguarding against any tampering of records. The alteration of audit trails or unauthorized access to healthcare data is strictly prohibited to maintain the sanctity of the process. Maintaining the integrity of the audit trail is essential for policy compliance assurance. If integrity is compromised, checking compliance status to find compliance and non-compliance cases is questionable. The blockchain provides these requirements as ledger properties. This work adopts private blockchain as an audit trail storage system.

Figure 5 illustrates the private audit blockchain's block components and structure. Each block has a block header part that contains block metadata and a data part that stores the audit trail data. Each audit trail has five components: *(i) audit trail ID; (ii) informed consent ID or SIC ID; (iii) honest broker ID; (iv) honest broker report;* and *(v) timestamp data.* The audit trail ID provides unique identifiers; the informed consent ID, or SIC ID, indicates the consent that is executed to share the intended PHI. From SIC ID, it is possible to get the components: sender, receiver, PHI, and purpose. The honest broker ID indicates which broker certifies or attests to the intended PHI's protection status (encryption or anonymity). Finally, the timestamp means the time when the sharing authorization is done. Steps *6a, 6b,* and *6c* in Figure

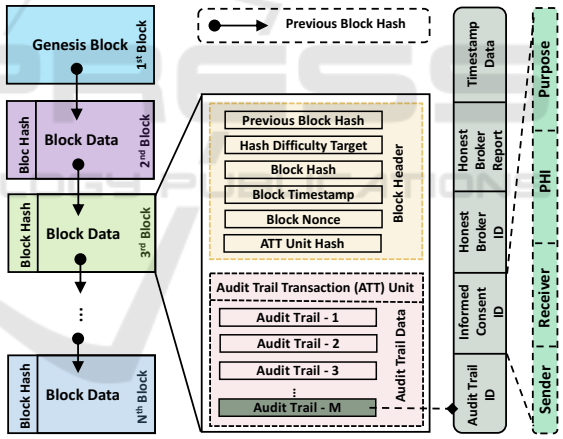

Figure 5: Audit Blockchain Block Structure.

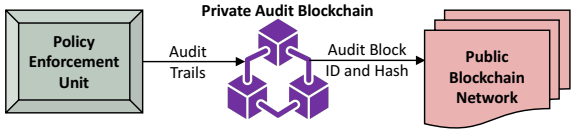

Figure 6: Storing Audit Blockchain Block ID and Hash.

4 show the process of capturing audit trails from the authorization module and honest broker.

Enforcement activity data is collected and stored in a private blockchain known as an audit blockchain as immutable records to ensure consent provenance and maintain compliance. The private blockchain network is managed and maintained by an author-

ity, which means reading and writing permissions are given to limited participants or users. In this case, the trust and transparency of the private blockchain are questionable. It doesn't provide a public eye to maintain trust and transparency. Storing audit trails on the public blockchain gives trust and transparency, which is another issue to consider. Firstly, audit trails contain sensitive information like user activities, and storing them on a public blockchain creates security and privacy concerns. Secondly, audit trails produce enormous amounts of data, which requires a lot of money to store on the public blockchain. This is not feasible from a business perspective, as it increases business operation and treatment costs and service charges.

To overcome the aforementioned issues, this research stores audit trail data on a private blockchain called the private audit blockchain. Then, it stores the private audit blockchain block ID and block hash as integrity on the public blockchain. Storing block ID and integrity requires a small cost and provides trust and transparency. Any modifications to private audit blockchain data can be detected by comparing the block's current and stored hashes with those on the public blockchain. Figure 6 shows the private and public blockchain relationship for storing audit block ID and integrity in a public blockchain like Ethereum. We have configured a private blockchain that is based on the Ethereum client (Samuel et al., 2021) with the necessary smart contracts and API for capturing and storing audit trail data in the audit blockchain.

5 COMPLIANCE VERIFICATION

Enforcing applicable policies and maintaining audit trails are not enough to ensure policy compliance. There must be some mechanism to check compliance status using deployed and enforced policies with audit trails. The compliance checker must be an independent and separate entity from the policy enforcer and audit trail unit. This paper proposes a blockchain consensus mechanism to perform compliance-checking operations on the audit trails using deployed sharing informed consents (SIC) and other applicable policies. The consensus mechanism, called Proof of Compliance (PoC), is governed by a set of independent, distributed, and decentralized auditor nodes. Section 3 discusses the sharing informed consent structure and deployment process as the smart contract in the public blockchain. Section 4 gives the audit trail capturing and storing mechanism.

Figure 7 depicts the transaction structure of the Proof of Compliance consensus mechanism. The PoC takes input from an audit trail that contains (i) audit trail ID, (ii) informed consent ID or SIC ID, (iii) honest broker ID, (iv) honest broker report, and (v) timestamp data. Applicable policy and sharing informed consent are retrieved from the policy repository and public blockchain to check the status of each audit trail. After verifying, each auditor node determines the compliance status for each transaction. There are three compliance statuses: (i) *compliant*, which indicates there are no security and privacy policy violations; (ii) *non-compliant* means there is a policy violation, and (iii) *non-determined* defines that required information is not available to check status.

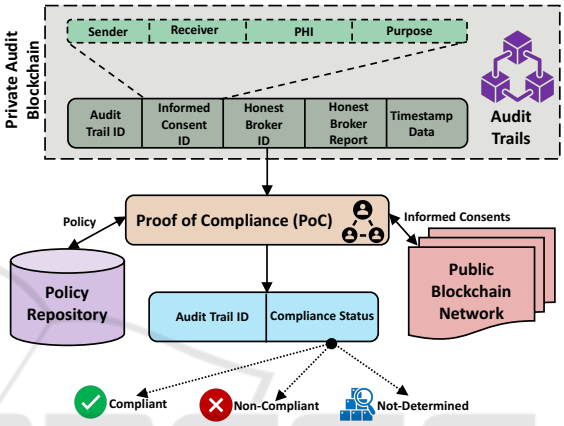

Figure 7: Proof of Compliance (PoC) Transaction Structure.

The auditor nodes can be hospitals, various governments, regulatory agencies, insurance companies, business associates, and others. They do not store audit trail data and are responsible for maintaining compliance status for each transaction. Reports from all auditor nodes are collected and combined for the final decision. Algorithm 2 shows the core functionalities of PoC: signature verification and order, transaction validation, policy compliance verification, and ledger modification. Due to page constraints, we do not include detailed protocols, communication mechanisms, and synchronization techniques. They are our future research communications with performance evaluations for compliance accuracy measurements, data security and privacy, and others.

6 SIC PROVENANCE SERVICES

Patients need to be provided with the specifics of their given sharing informed consent: who can share what PHI with whom, and for what purposes? Additionally, patients should understand the execution of their consent, including the details of who shares which healthcare data, the timing of these actions, and others. They should also know whether those sharing

Algorithm 2: Proof of Compliance (PoC) Consensus Method.

Input : (i) list of transactions ($Txns$) and (ii) set of policy $Plcy$
Output: (i) list of accepted/rejected transactions ($Txns$) and (ii) list of transactions that are policy compliance

Initialization (i) $\mathbb{N}_{Order}$: order nodes, (ii) $\mathbb{N}_{Validator}$: validator/endorser nodes, (iii) $\mathbb{N}_{Audit}$: audit nodes, and (iv) $\mathbb{N}_{Committer}$: committer nodes
Signature Verification and Order
$Txn_{Valid} = []$ /* accepted transaction list */
$Txn_{Invalid} = []$ /* rejected transaction list */
for $i \leftarrow Txns_{Start}$ **to** $Txns_{End}$ **by** 1 **do**
  if $\zeta(PK_i, Tnx_i) == Signed_{Tnx_i}$ **then**
    $Txn_{Valid} \leftarrow Txn_{Valid} + Txn_i$
  else
    $Txn_{Invalid} \leftarrow Txn_{Invalid} + Txn_i$
  end if
end for
Transaction Validation $Txn_{Accepted} = []$ /* accepted transaction list */
$Txn_{Rejected} = []$ /* rejected transaction list */
for $i \leftarrow Txn_{Valid\,Start}$ **to** $Txn_{Valid\,End}$ **by** 1 **do**
  if $\zeta(PK_i, Tnx_i) == Signed_{Tnx_i}$ **then**
    $Txn_{Accepted} \leftarrow Txn_{Accepted} + Txn_{Valid\,i}$
  else
    $Txn_{Rejected} \leftarrow Txn_{Rejected} + Txn_{Valid\,i}$
  end if
end for
Policy Compliance Verification
$Txn_{Compliance} = []$ /* compliance transactions */
$Txn_{NonCompliance} = []$ /* noncompliance transactions */
for $i \leftarrow Txn_{Accepted\,Start}$ **to** $Txn_{Accepted\,End}$ **by** 1 **do**
  if $\zeta(PK_i, Tnx_i) == Signed_{Tnx_i}$ **then**
    $Txn_{Compliance} \leftarrow Txn_{Compliance} + Txn_{Accepted_i}$
  else
    $Txn_{NonCompliance} \leftarrow Txn_{NonCompliance} + Txn_{Accepted_i}$
  end if
end for
Ledger Modification
$Txn_{Compliance} = []$ /* compliance transactions */
$Txn_{NonCompliance} = []$ /* noncompliance transactions */
for $i \leftarrow Txn_{Accepted\,Start}$ **to** $Txn_{Accepted\,End}$ **by** 1 **do**
  if $\zeta(PK_i, Tnx_i) == Signed_{Tnx_i}$ **then**
    $Txn_{Compliance} \leftarrow Txn_{Compliance} + Txn_{Accepted_i}$
  else
    $Txn_{NonCompliance} \leftarrow Txn_{NonCompliance} + Txn_{Accepted_i}$
  end if
end for

activities comply with the applicable security and privacy policies, regulatory requirements, industry best practices, contractual obligations, etc. This section outlines the services related to the given and executed consent that patients can access within the proposed framework, provided they have the necessary credentials. The primary goal of provenance services is to ensure patients receive accurate and comprehensive information and have confidence regarding their given and executed informed consent.

6.1 Given Consent Services

In this scope, patients can access the list of all the given consents for sharing healthcare data to date. These consents are in their original state and may or may not be executed for making data-sharing decisions. Patients can see the list where each consent contains information about who the sender is, who the receiver is, what the protected healthcare information is, and the purpose of sharing healthcare data when the sharing informed consent is given. Given consent services can be delivered: *(i) sender-oriented, (ii) receiver-oriented, (iii) PHI-oriented,* and *(iv) purpose-oriented.* For example, patients can have sender-oriented consent services that include all the consents given to a particular sender or a group of senders. Figure 8 depicts sender-oriented given consents for Donald, who has permission to share PHI with various receivers. Figure 9 shows the PHI-oriented given consents for health record *PHI-1008*.

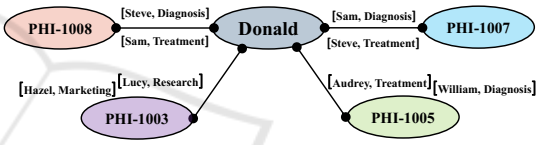

Figure 8: Sender-oriented Given Consents.

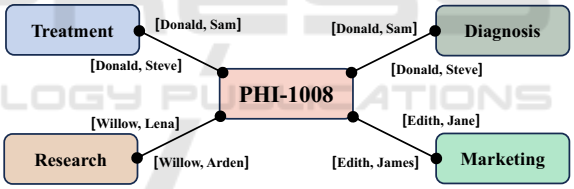

Figure 9: PHI-Oriented Given Consents.

6.2 Executed Consent Services

After generation, all consents may or may not be executed to share healthcare data. A consent is executed when a sender wants to share PHI with the receiver when there is a need that serves the purpose included in the consent. If consent is executed, other information is stored in addition to the consent, like an honest broker ID, a pertinent policy status that the broker has certified, a timestamp, etc. Executed consent services can be provided: *(i) sender-oriented, (ii) receiver-oriented, (iii) PHI-oriented,* and *(iv) purpose-oriented.* For example, a patient may need to know the executed consent for a particular receiver. Figure 10 shows receiver-oriented executed consents for *Steve* with senders and timestamps. Figure 11 depicts purpose-oriented executed consents for *treatment* with sender, receiver, and timestamp.

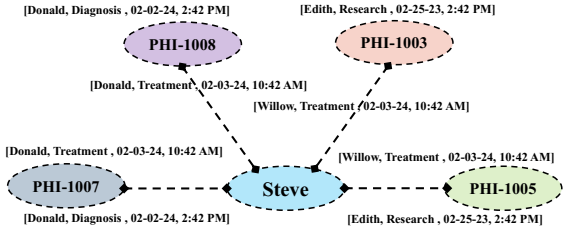

Figure 10: Receiver-oriented Executed Consents.

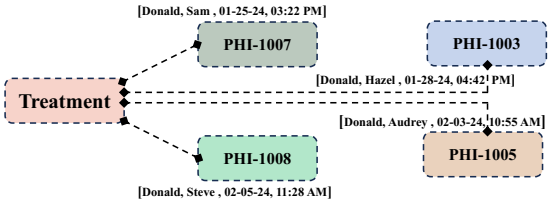

Figure 11: Purpose-oriented Executed Consents.

6.3 Service Delivery to Patients

Patients will interact with the system through interfaces like GUIs or apps supported by wallets like *Coinbase* and *MetaMask* for transaction signing and data access management. These wallets safeguard users' private keys and credentials. The system accommodates various user types, including those requiring tailored interfaces, such as seniors, physically disabled individuals, minors, and others. Healthcare providers may address the specific needs of these diverse users and can develop apps and software to provide services. Patients' devices and apps are assumed to be secure against unauthorized access, and communication with the blockchain is also protected.

7 EXPERIMENTAL EVALUATION

The Ethereum Virtual Machine (EVM) based three blockchain test networks (*Arbitrum*, *Polygon*, and *Optimism*) are chosen for the experiments. We developed and deployed smart contracts for storing and retrieving PPA integrity and informed consent in test networks. Ethereum's Remote Procedure Call (RPC) API services are employed for deploying smart contracts and performing transactions on these networks (Kim and Hwang, 2023). Utilizing public *RPC* eliminates the need to maintain a blockchain node for contract interaction, assuming minimal resource usage (CPU, HDD, bandwidth) on the local machine. We used Metamask wallet to sign and authorize transactions using *ETH* and *MATIC* faucet tokens as gas. Healthcare providers may invest in infrastructure such as blockchain nodes, web interfaces, and mobile applications for seamless service interaction between patients and healthcare systems. Storing informed consent on public blockchains like Ethereum incurs direct monetary costs. Patients, insurance companies, and others can split these costs, like those for doctor visits, medications, and laboratory tests. The following discusses gas consumption and time requirements.

7.1 Gas Consumption

Gas is needed for any activity on the Ethereum network involving writing data or changing the state of the blockchain. Smart contract deployment and function calling costs to write data on the blockchain network are considered in this work. A contract is deployed for each patient separately to manage consent-related queries efficiently. The cost of smart contract deployment is proportional to the size of the code (Albert et al., 2020). This is a one-time cost for a single-contract deployment. How much it costs to call a function depends on how many times it is called and how much data needs to be stored or changed on the blockchain network. Figure 12, 13, 14, 15, and 16 show the contract deployment and consent storage costs in gas (token) and USD for three test networks.

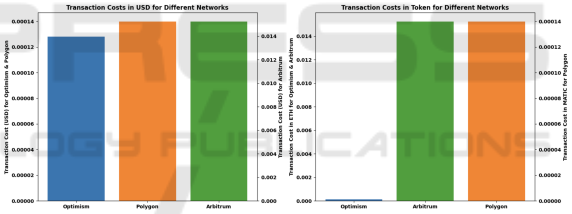

Figure 12: PPA Integrity Storage Cost.

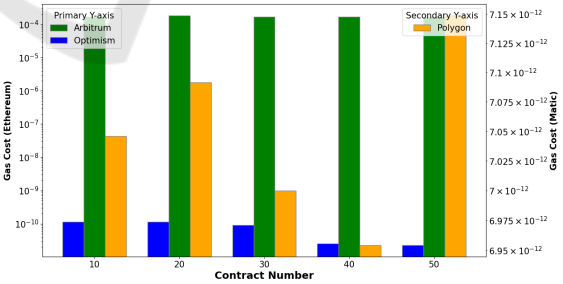

Figure 13: Contract Deployment Gas Cost.

7.2 Time Requirements

Blockchain-based applications require block data writing and reading time requirements. Writing time includes smart contract deployment and data addition. Table 3 shows the writing time for various consent numbers for the test networks. The reading time indicates the required time to get data from the block

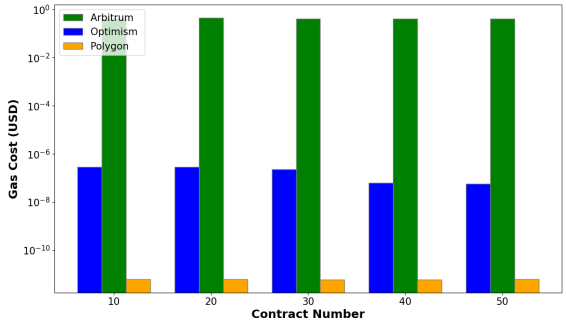

Figure 14: Contract Deployment USD Cost.

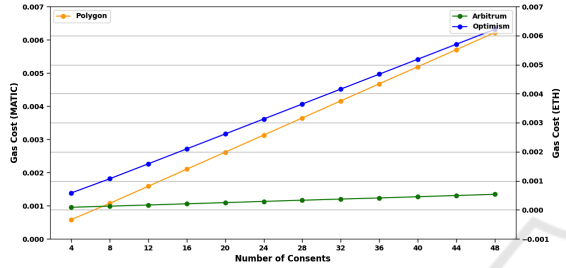

Figure 15: Consent Storage Gas Cost.

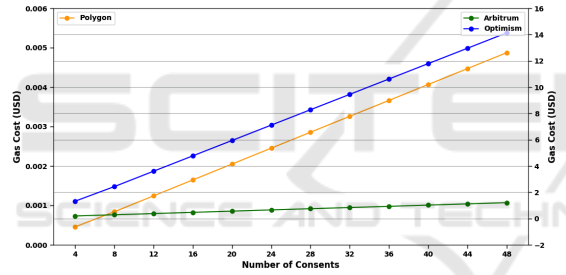

Figure 16: Consent Storage USD Cost.

of the blockchain ledger. All the read calls of smart contracts are gas-free. Table 4 shows the test network's reading time for various consent numbers. The same smart contracts and consents are used for all test networks. Maintaining a node locally can reduce the reading time from the network where block data can be accessed in real-time. The system continuously synchronizes with the blockchain network to update the ledger data. The providers can maintain local nodes for faster authorizations.

8 CONCLUSIONS

Sharing patient health data is beneficial for improving medical care, diagnosis, and other essential services. However, keeping this information private and secure is important. Different policies from various authorities help ensure the privacy and security of this health data. Complying with these policies ensures that safety measures are working. Getting patients' informed consent is also critical to protecting their privacy and giving them control over sharing their information. Patients need to understand fully how their data is shared. Patients should also feel confident that strong safeguards are in place to protect their data. Using smart contracts to manage patient consent is a promising way to securely and privately share health data. These systems let patients control their health records and agree to how doctors and others use them. Blockchain technology improves these systems by providing security, efficiency, decentralization, transparency, and immutability. This enhances the trustworthiness and responsibility of sharing healthcare data among everyone involved.

Looking forward, our objective is to provide functional mechanisms for essential consent management operations for data sharing and enhancing patient care and services. Management operations generate, modify, withdraw, expire, and archive consent. Improper consent can cause sensitive data disclosure or prevent getting services. Consent generation must be done carefully. It is necessary to modify a given consent due to improper components like the receivers or purposes. In this situation, a modified new consent must be deployed, while the old consent must be moved to the achieving repository.

Table 3: Consent Writing Time to Blockchain Network.

Consents #	Polygon	Arbitrum	Optimism
4	6.719 Sec	6.854 Sec	8.459 Sec
8	5.961 Sec	6.068 Sec	7.785 Sec
12	5.972 Sec	6.338 Sec	7.738 Sec
16	6.309 Sec	6.063 Sec	7.762 Sec
20	6.085 Sec	6.081 Sec	8.163 Sec
24	6.015 Sec	2.476 Sec	7.482 Sec
28	10.117 Sec	6.521 Sec	7.718 Sec
32	10.041 Sec	2.451 Sec	8.268 Sec
36	10.045 Sec	6.662 Sec	7.736 Sec
40	14.039 Sec	2.458 Sec	7.797 Sec
44	10.048 Sec	6.201 Sec	7.881 Sec
48	10.138 Sec	6.174 Sec	8.971 Sec

Table 4: Consent Reading Time from Blockchain Network.

Consents #	Polygon	Arbitrum	Optimism
4	0.426 Sec	0.234 Sec	0.399 Sec
8	0.366 Sec	0.201 Sec	0.423 Sec
12	0.337 Sec	0.239 Sec	0.425 Sec
16	0.346 Sec	0.259 Sec	0.423 Sec
20	0.327 Sec	0.288 Sec	0.442 Sec
24	0.344 Sec	0.241 Sec	0.579 Sec
28	0.358 Sec	0.221 Sec	0.536 Sec
32	0.361 Sec	0.288 Sec	0.495 Sec
36	0.401 Sec	0.225 Sec	0.512 Sec
40	0.36 Sec	0.206 Sec	0.482 Sec
44	0.361 Sec	0.233 Sec	0.462 Sec
48	0.522 Sec	0.224 Sec	0.434 Sec

ACKNOWLEDGEMENTS

This work was partially supported by the U.S. National Science Foundation under Grant No. 1822118 and 2226232, the member partners of the NSF IUCRC Center for Cyber Security Analytics and Automation – Statnett, AMI, NewPush, Cyber Risk Research, NIST, and ARL – the State of Colorado (grant #SB 18-086), and the authors' institutions. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation or other organizations and agencies.

REFERENCES

Al Amin, M., Altarawneh, A., and Ray, I. (2023). Informed consent as patient driven policy for clinical diagnosis and treatment: A smart contract based approach. In *Proceedings of the 20th International Conference on Security and Cryptography-SECRYPT*, pages 159–170.

Alarcon, M. L., Nguyen, M., Debroy, S., Bhamidipati, N. R., Calyam, P., and Mosa, A. (2021). Trust model for efficient honest broker based healthcare data access and processing. In *2021 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops)*, pages 201–206. IEEE.

Albert, E., Correas, J., Gordillo, P., Román-Díez, G., and Rubio, A. (2020). Gasol: Gas analysis and optimization for ethereum smart contracts. In *International Conference on Tools and Algorithms for the Construction and Analysis of Systems*, pages 118–125. Springer.

Alhajri, M., Salehi Shahraki, A., and Rudolph, C. (2022). Privacy of fitness applications and consent management in blockchain. *Proceedings of the 2022 Australasian Computer Science Week*, pages 65–73.

Aljabri, M., Aldossary, M., Al-Homeed, N., Alhetelah, B., Althubiany, M., Alotaibi, O., and Alsaqer, S. (2022). Testing and exploiting tools to improve owasp top ten security vulnerabilities detection. In *2022 14th International Conference on Computational Intelligence and Communication Networks (CICN)*, pages 797–803. IEEE.

Amofa, S., Sifah, E. B., Kwame, O.-B., Abla, S., Xia, Q., Gee, J. C., and Gao, J. (2018). A blockchain-based architecture framework for secure sharing of personal health data. In *2018 IEEE 20th international conference on e-Health networking, applications and services (Healthcom)*, pages 1–6. IEEE.

Balistri, E., Casellato, F., Giannelli, C., and Stefanelli, C. (2021). Blockhealth: Blockchain-based secure and peer-to-peer health information sharing with data protection and right to be forgotten. *ICT Express*, 7(3):308–315.

Buterin, V. et al. (2014). A next-generation smart contract and decentralized application platform. *white paper*, 3(37):2–1.

Chung, K., Chung, D., and Joo, Y. (2006). Overview of administrative simplification provisions of hipaa. *Journal of medical systems*, 30:51–55.

Fan, K., Wang, S., Ren, Y., Li, H., and Yang, Y. (2018). Medblock: Efficient and secure medical data sharing via blockchain. *Journal of medical systems*, 42(8):136.

Hutchings, E., Loomes, M., Butow, P., and Boyle, F. M. (2021). A systematic literature review of attitudes towards secondary use and sharing of health administrative and clinical trial data: a focus on consent. *Systematic Reviews*, 10:1–44.

Kim, S. and Hwang, S. (2023). Etherdiffer: Differential testing on rpc services of ethereum nodes. In *Proceedings of the 31st ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering*, pages 1333–1344.

Le, T.-V. and Hsu, C.-L. (2021). A systematic literature review of blockchain technology: Security properties, applications and challenges. *Journal of Internet Technology*, 22(4):789–802.

Lopez Martinez, A., Gil Pérez, M., and Ruiz-Martínez, A. (2023). A comprehensive review of the state-of-the-art on security and privacy issues in healthcare. *ACM Computing Surveys*, 55(12):1–38.

Mulamba, D. and Ray, I. (2017). Resilient reference monitor for distributed access control via moving target defense. In *Data and Applications Security and Privacy XXXI: 31st Annual IFIP WG 11.3 Conference, DBSec 2017, Philadelphia, PA, USA, July 19-21, 2017, Proceedings 31*, pages 20–40. Springer.

Rights (OCR), O. f. C. (2008). HIPAA Enforcement. Last Modified: 2021-06-28T08:59:34-0400.

Samuel, C. N., Glock, S., Verdier, F., and Guitton-Ouhamou, P. (2021). Choice of ethereum clients for private blockchain: Assessment from proof of authority perspective. In *2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pages 1–5. IEEE.

Shah, M., Li, C., Sheng, M., Zhang, Y., and Xing, C. (2019). Crowdmed: A blockchain-based approach to consent management for health data sharing. In *Smart Health: International Conference, ICSH 2019, Shenzhen, China, July 1–2, 2019, Proceedings 7*, pages 345–356. Springer.

Timmermans, S. (2020). The engaged patient: The relevance of patient–physician communication for twenty-first-century health. *Journal of Health and Social Behavior*, 61(3):259–273.

Zhuang, Y., Sheets, L. R., Chen, Y.-W., Shae, Z.-Y., Tsai, J. J., and Shyu, C.-R. (2020). A patient-centric health information exchange framework using blockchain technology. *IEEE journal of biomedical and health informatics*, 24(8):2169–2176.