Original Paper

Identity-Centric Blockchain Framework for Medical Imaging Data Governance in Intensive Care Unit Patients With COVID-19–Associated Acute Respiratory Distress Syndrome: Development and Usability Study

Elder Bruno Evaristo Correa Sr[1,2]; João Carlos Amaro Ferreira Sr 2nd[3,4,5]; Antonio Jorge Gomes Abelém Sr 3rd[6]

[1]Graduate Program in Computer Science, Universidade Federal do Pará, Belém, Pará, Brazil
[2]Centre for Research and Development in Telecommunications (Brazil), Campinas, São Paulo, Brazil
[3]Molde University College, Molde, Møre og Romsdal, Norway
[4]Iscte – Instituto Universitário de Lisboa, Lisboa, Lisbon, Portugal
[5]Instituto de Novas Tecnologias, Lisboa, Lisbon, Portugal
[6]Universidade Federal do Pará, Belém, Pará, Brazil

Corresponding Author:

João Carlos Amaro Ferreira Sr 2nd
Molde University College
Britvegen 2
Molde, Møre og Romsdal 6410
Norway
Phone: 47 71 21 40 00
Email: joam@himolde.no

Abstract

Background: The management of multimodal health data in intensive care units (ICUs) remains a significant challenge due to system fragmentation, reliance on manual consent processes, and limited mechanisms for patient-controlled data access.

Objective: This study aimed to propose and validate a patient-centric framework integrating Fast Healthcare Interoperability Resources (FHIR) with blockchain-based BioWallets, a Flutter-based BioWallet application developed by the authors, and an identity-centric governance model. A key novelty is the decoupling of governance logic from ledger execution, whereby identity verification and policy evaluation are executed off-chain, while only cryptographic commitments are anchored on-chain.

Methods: Following the design science research methodology, the framework was implemented using HAPI FHIR, Hyperledger Besu, InterPlanetary File System (IPFS), and a cross-platform BioWallet and was evaluated across 110 pseudonymized ICU patients (220 chest radiographs). Usability findings were preliminary and exploratory (n=5).

Results: There was a 67% (from 125.4 to 41.2 s) reduction in data access latency. The mean smart contract consent verification time was 1.73 (SD 0.31, 95% CI 1.64-1.82) seconds. Under controlled conditions using 5 author-defined attack scenarios derived from STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege) threat modeling, all simulated unauthorized access attempts were blocked (5/5); independent penetration testing remains a prerequisite before any clinical deployment. The identity-centric governance function was exercised across all 30 evaluated transactions (25 authorized and 5 blocked), with each predicate (identity, policy, authorization, and integrity) logged and operating as specified across the evaluated scenarios. Exploratory usability mean scores (n=5, 5-point Likert scale) were 4.6 for ease of use, 4.8 for perceived security, and 4.4 for preference over existing systems; qualitative feedback highlighted the clarity of the consent-management interface and the perceived value of patient-mediated access control in time-critical scenarios. All findings are bounded by the proof-of-concept scope and require multicenter validation for generalizability.

Conclusions: The framework demonstrates technical feasibility for ICU data governance. Broader scalability and generalizability claims await multicenter validation.

JMIR Form Res 2026;10:e99002; doi: 10.2196/99002

Keywords: blockchain; digital health wallet; Fast Healthcare Interoperability Resources; FHIR; medical imaging; acute respiratory distress syndrome; ARDS; health data governance; COVID-19; decentralized consent; interoperability; decentralized identity

Introduction

Background and Rationale

The complexity of health data management in intensive care environments has increased significantly, particularly for patients with severe conditions such as acute respiratory distress syndrome (ARDS) associated with COVID-19 [1,2]. Traditional clinical workflows rely on fragmented electronic health records (EHRs), picture archiving and communication systems (PACS), laboratory systems, and bedside monitoring devices, often requiring manual data extraction and paper-based consent mechanisms [3]. These limitations hinder timely clinical decision-making and compromise the assembly of longitudinal multimodal datasets essential for both patient care and scientific research [4,5]. Fast Healthcare Interoperability Resources (FHIR) provides a modular, resource-based standard that supports real-time exchange of structured data across heterogeneous systems [6]. However, FHIR primarily addresses technical interoperability and does not inherently resolve issues related to patient consent, data provenance, privacy governance, or interinstitutional data sharing [7]. In parallel, blockchain technologies, through the use of decentralized identifiers (DIDs), verifiable credentials (VCs), and smart contracts, offer cryptographic security, immutable audit trails, and mechanisms for patient-controlled data access [8,9].

Recent literature on blockchain network governance indicates that ledger-centric models tightly coupled with on-chain execution have limitations in scalability, interoperability, and flexibility. In contrast, identity-centric architectures enable the decoupling of governance logic into an off-chain control plane, where decentralized identities, VCs, and explicit policy rules are evaluated before anchoring only cryptographic commitments and final decision outcomes on-chain [10]. This decoupling is particularly well suited for high-sensitivity clinical scenarios where privacy, latency, and traceability must coexist.

The central research question guiding this study is how can a blockchain-enabled, FHIR-compliant architecture incorporating digital health wallets and an identity-centric governance layer facilitate secure, patient-controlled, and timely access to clinical and imaging data for intensive care unit (ICU) patients with ARDS due to COVID-19?

The main contributions of this work are as follows:

- Development of a patient-centric framework to integrate FHIR standards, BioWallets, and identity-centric governance for the secure and interoperable management of medical imaging and clinical data.
- Implementation of decentralized consent management using VCs, DIDs, smart contracts, and off-chain policy evaluation to ensure transparent access control and General Data Protection Regulation (GDPR) compliance.
- Integration of longitudinal, multimodal datasets from ICU patients with ARDS/COVID-19 to support structured research and predictive analytics.
- Design of a scalable architecture in which the blockchain functions as a semantic governance anchor to preserve privacy and patient autonomy by minimizing on-chain exposure of sensitive data.
- Validation of the framework through a prototype and a simulated ICU case study to demonstrate the feasibility of longitudinal monitoring of ARDS progression in patients with COVID-19.

The remainder of this manuscript is organized as follows. The *Literature Review* section reviews the related literature. The *Methods* section details the methodology, governance model, and threat-modeling approach. The *Results* section presents implementation, validation, and security evaluation outcomes. The *Discussion* section discusses the findings. The *Conclusions* section concludes the paper.

Literature Review

Literature Search Strategy

This systematic literature review was conducted and reported in accordance with the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) 2020 guidelines [11], ensuring methodological transparency, reproducibility, and rigor. The primary objective was to systematically identify, critically evaluate, and synthesize peer-reviewed evidence on the integration of blockchain technology, FHIR, decentralized identity frameworks, and digital health wallets for the secure, interoperable, and privacy-preserving management of medical imaging and clinical data. Particular emphasis was placed on applications relevant to intensive care environments and ARDS/COVID-19 scenarios, where timely access, data integrity, and governance are critical.

A comprehensive and reproducible search strategy was developed in consultation with domain-specific terminology and indexing standards. Searches were conducted across 5 major electronic databases: PubMed/MEDLINE, Scopus, IEEE Xplore, Web of Science, and the Association for Computing Machinery (ACM) Digital Library, covering the period from January 1, 2018, to March 31, 2025. This time frame was selected to capture the rapid evolution of blockchain-enabled health care architectures and the emergence of FHIR-based interoperability solutions. The search strategy combined controlled vocabulary (eg, MeSH terms) with free-text keywords and Boolean operators, including combinations of terms such as “blockchain,” “FHIR,” “electronic health records,” “medical imaging,” “digital health wallet,” “decentralized identifier,” “verifiable credential,” and “consent management.” Where applicable, database-specific syntax and filters were applied to maximize recall and precision.

Eligibility criteria were defined a priori. Studies were included if they (1) were peer-reviewed and published in English; (2) described technical architectures, system integrations, prototypes, or frameworks involving blockchain and/or FHIR; and (3) reported either empirical results, implementation details, or evaluation outcomes. Studies focusing solely on theoretical discussions, without architectural or technical contributions, were excluded. Additional exclusion criteria comprised gray literature (eg, reports and white papers), preprints, editorials, and studies unrelated to health care applications or lacking relevance to data interoperability, security, or governance.

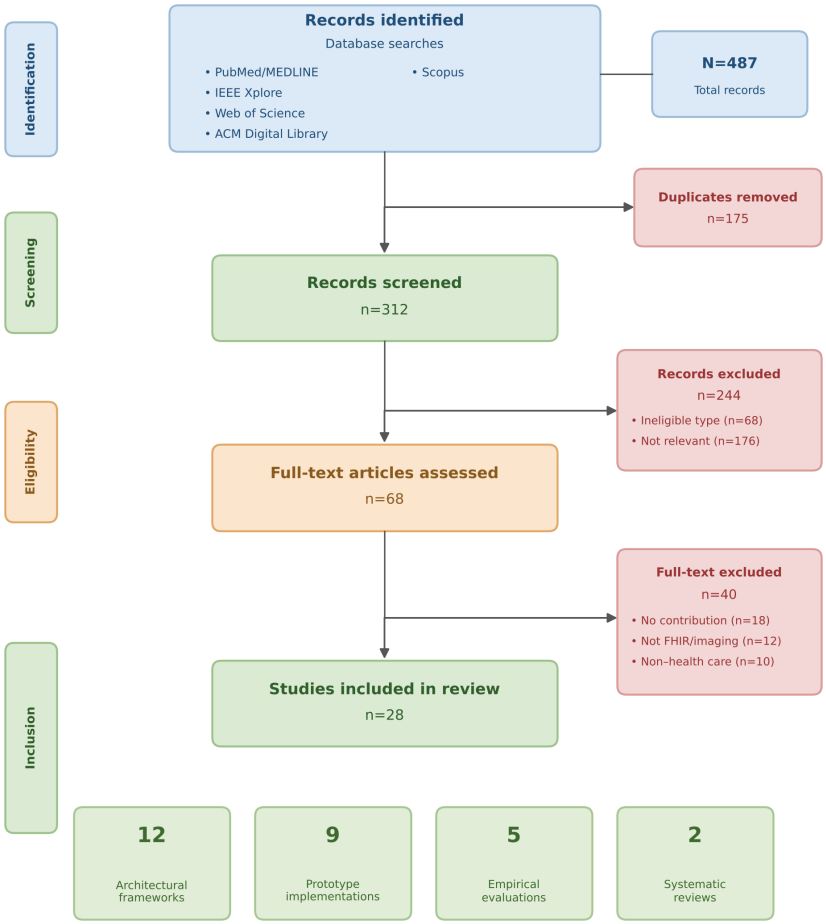
All retrieved records were imported into Rayyan (QCRI) for systematic management, duplicate removal, and screening. A 2-stage screening process was conducted. In the first stage, 2 independent reviewers assessed titles and abstracts for relevance. In the second stage, full-text articles were evaluated against predefined inclusion and exclusion criteria. Discrepancies between reviewers were resolved through discussion and consensus, ensuring consistency in study selection. Interreviewer agreement was qualitatively monitored throughout the process.

Data extraction was performed using a structured template to ensure consistency and completeness. Extracted variables included publication year, study design, application domain, blockchain platform (eg, Ethereum-based and Hyperledger), use of FHIR resources, identity management approaches (eg, DIDs and VCs), data storage strategies (on-chain vs off-chain), security and privacy mechanisms, evaluation metrics (eg, latency, scalability, and access control effectiveness), and key findings. Particular attention was given to how studies addressed interoperability, consent management, auditability, and governance.

The synthesis of results was conducted qualitatively, focusing on identifying recurring architectural patterns, technological trends, and research gaps. Studies were categorized based on their primary contribution (eg, architectural frameworks, prototype implementations, empirical evaluations, or reviews). The analysis also examined the extent to which existing solutions addressed the challenges of multimodal data integration, patient-centric control, and scalable governance in high-sensitivity clinical environments such as ICUs.

Figure 1 presents the PRISMA 2020 flow diagram. Of 487 identified records, 175 duplicates were removed. After title/abstract screening (n=312) and full-text review (n=68), 28 studies were included in the qualitative synthesis (excluded: n=18, lack of empirical contribution; n=12, no FHIR/imaging focus; n=10, non–health care applications).

Figure 1. PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) 2020 flow diagram. FHIR: Fast Healthcare Interoperability Resources.



Synthesis of Findings

The 28 included studies consisted of 12 framework or architectural papers, 9 prototype implementations, 5 empirical evaluations or pilot studies, and 2 systematic reviews. The majority (n=19, 68%) were published between 2022 and 2025. Permissioned ledgers (Ethereum-compatible or Hyperledger) were most common; FHIR was explicitly integrated into 21 studies, primarily through Consent, DiagnosticReport, Observation, and Patient resources.

Data Fragmentation and Interoperability

Several studies confirmed persistent fragmentation across EHRs, PACS, laboratory systems, and monitoring devices, leading to delays and incomplete longitudinal datasets in ICU settings [3,12,13]. Although FHIR has advanced technical interoperability [6,14], semantic harmonization, consent governance, and interinstitutional data provenance remain significant challenges for multimodal ARDS cohorts [7,15].

Blockchain Applications in Health Data Management

Blockchain has been consistently positioned as a complementary integrity layer providing cryptographic immutability, automated consent enforcement, and decentralized trust [8,9,16]. Prior prototypes have reported near-complete prevention of unauthorized access, tamper-proof audit trails, and improved reproducibility in clinical research, particularly when combined with encrypted off-chain storage solutions [17-19].

Decentralized Identity, BioWallets, and Consent Management

Decentralized identity systems and BioWallets have been proposed as a means of supporting patient data sovereignty [8,20-22]. Patient-controlled wallets storing DIDs and VCs enable selective, revocable sharing of clinical and imaging data without reliance on centralized intermediaries [21]. Integration with FHIR resources facilitates seamless data exchange across institutions while preserving privacy [22].

Identity-Centric Governance Beyond Ledger-Centric Models

Recent work on federated blockchain governance argues that machine-readable governance rules can be executed off-chain, with identity and credential verification performed by decentralized agents, while the blockchain is limited to anchoring cryptographic commitments and final decision outcomes [10]. This approach enhances privacy, scalability, and interoperability compared with DAO-centric and consensus-centric models and provides a valuable conceptual framework for multi-institutional clinical ecosystems.

Blockchain-FHIR Integration for Clinical Research

Architectures such as FHIRChain and HealthChain have demonstrated the feasibility of encapsulating FHIR resources within blockchain transactions for secure and scalable data sharing [19,23]. However, scalability, transaction latency, and regulatory acceptance remain ongoing challenges [20].

Research Gaps and Rationale

Four critical gaps remain in the literature: limited application to medical imaging datasets; absence of end-to-end frameworks integrating FHIR ingestion, encrypted off-chain storage, BioWallets, and full consent lifecycle management; lack of validation in ICU simulation environments with quantitative metrics for latency, security, and usability; and limited explicit incorporation of identity-centric governance decoupled from ledger execution. This study directly addresses all 4 gaps.

Methods

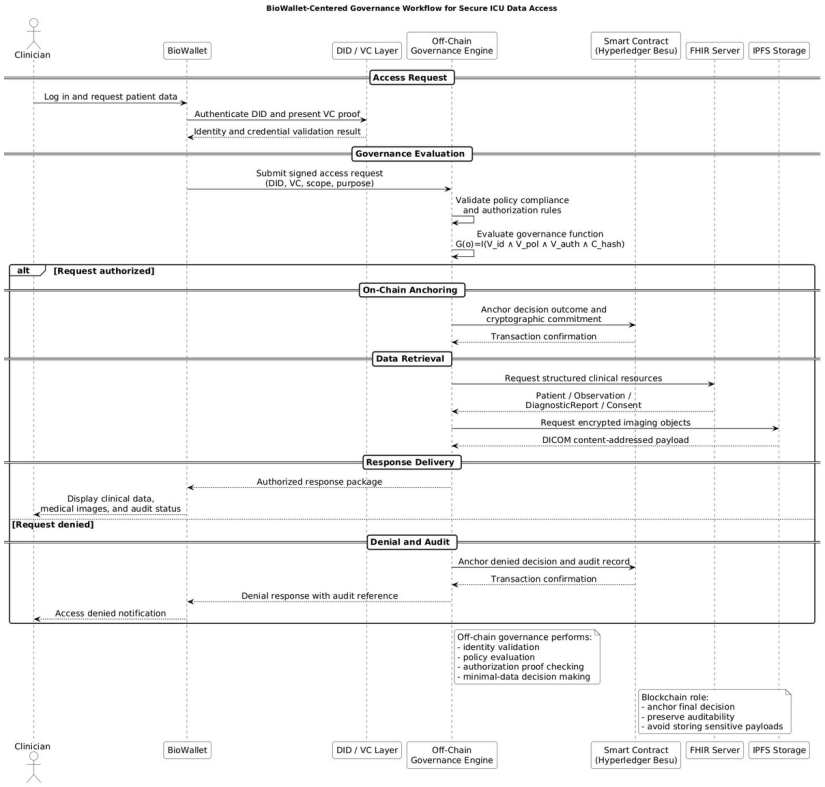
Study Design

This study followed the design science research (DSR) methodology [24,25] to develop and evaluate a patient-centric framework for secure, interoperable, and privacy-preserving management of medical imaging and clinical data in intensive care settings. DSR was selected because it emphasizes the creation of innovative artifacts that solve real-world problems while contributing new knowledge. The research process comprised 5 iterative phases: problem identification and motivation, definition of solution objectives, artifact design and development, demonstration and evaluation, and communication of results.

Framework Architecture

The proposed framework comprises 4 tightly integrated layers that collectively enable the end-to-end governance workflow illustrated in Figure 2. The first layer is a FHIR-compliant data integration layer that ingests, standardizes, and harmonizes multimodal clinical and imaging data, exposing standardized resources such as Patient, Observation, DiagnosticReport, and Consent. The second layer is a permissioned blockchain infrastructure (Hyperledger Besu) functioning as a semantic governance anchor, recording only cryptographic commitments, minimal metadata, and final decision outcomes after governance evaluation. The third layer is the BioWallet client (mobile and web application) that enables patient-mediated access control through DIDs, VCs, and biometric authentication. The fourth layer is an encrypted off-chain storage infrastructure based on InterPlanetary File System (IPFS; Protocol Labs) for large clinical payloads, including Digital Imaging and Communications in Medicine (DICOM) imaging data, with Advanced Encryption Standard (AES)-256 encryption.

Figure 2. Sequence diagram of the governance workflow in the proposed framework. The framework separates clinical data management from off-chain governance and uses blockchain for decision anchoring and auditability. DICOM: Digital Imaging and Communications in Medicine; DID: decentralized identifier; FHIR: Fast Healthcare Interoperability Resources; IPFS: InterPlanetary File System; VC: verifiable credential.



The interaction among layers follows a structured sequence: (1) authentication via DID/VC verification; (2) submission of a signed access request; (3) off-chain governance evaluation; (4) on-chain anchoring of the decision outcome; and (5) controlled retrieval of clinical and imaging data from FHIR and IPFS services, as illustrated in Figure 2. This architecture ensures compliance with GDPR requirements for data minimization, consent revocation, and patient autonomy [26].

Identity-Centric Governance Model

An off-chain control plane for machine-readable governance was introduced. Decentralized identity agents validate DIDs, VCs, access policies, request scope, and authorization proofs prior to any on-chain write operations. The blockchain serves as a semantic anchor, recording only cryptographic commitments, minimal metadata, and final governance decision outcomes [10]. The governance decision is formalized as a deterministic function:

$$G(o) = V_{\text{id}}(o) \wedge V_{\text{pol}}(o) \wedge V_{\text{auth}}(o) \wedge C_{\text{hash}}(o) \quad (1)$$

Here $V_{\text{id}}(o)$ denotes identity validation, $V_{\text{pol}}(o)$ represents compliance with applicable access policies, $V_{\text{auth}}(o)$ corresponds to the authorization proof associated with the request, and $C_{\text{hash}}(o)$ denotes the cryptographic commitment of the relevant data artifacts. The function G returns a valid governance decision only if all conditions are satisfied.

This formulation ensures that governance decisions are evaluated deterministically and consistently across distributed environments. By requiring simultaneous validation of identity, policy compliance, authorization, and data integrity, the model enforces strict access controls while preserving auditability and nonrepudiation. Only the final decision outcome and its associated cryptographic commitment are anchored on-chain, whereas identity verification and policy evaluation remain off-chain, thereby reducing computational overhead and minimizing exposure of sensitive data.

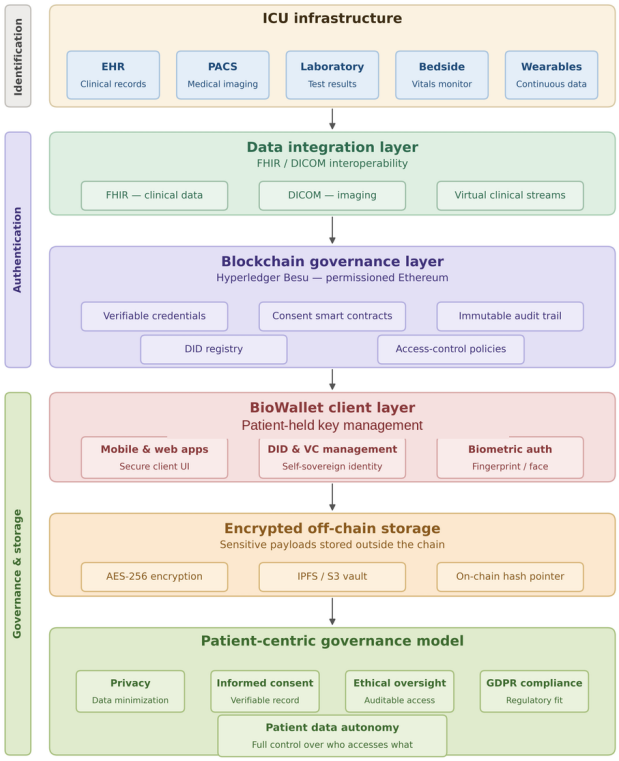
This decoupling reduces on-chain complexity, limits exposure of sensitive information, and enables flexible evolution of access control policies without requiring frequent smart contract redesign. The BioWallet serves as the patient-facing interface for issuing, presenting, and revoking credentials, while the FHIR server and IPFS collectively constitute the clinical data plane.

Dataset

Figure 3 shows that the framework was validated using a curated and pseudonymized dataset derived from 110 adult ICU patients with COVID-19–induced ARDS. Each patient record included 2 chest radiographs (220 DICOM images in total), along with structured longitudinal clinical metadata, including oxygenation indices, ventilatory parameters, comorbidities, laboratory markers, therapeutic interventions, and clinical outcomes. This dataset is appropriate for a DSR proof-of-concept, with the objective of demonstrating that the artifact functions as intended across all framework components [24,25]. Broader claims of generalizability require

multicenter validation with larger datasets (see *Residual Risks*).

Figure 3. Patient-centric governance architecture integrating intensive care unit (ICU) infrastructure, data interoperability, blockchain governance, patient-held identity management, encrypted off-chain storage, and governance controls. AES: Advanced Encryption Standard; DICOM: Digital Imaging and Communications in Medicine; DID: decentralized identifier; EHR: electronic health record; FHIR: Fast Healthcare Interoperability Resources; GDPR: General Data Protection Regulation; IPFS: InterPlanetary File System; PACS: picture archiving and communication systems; S3: Simple Storage Service; UI: user interface; VC: verifiable credential.



Data Preparation and Standardization

All personally identifiable information was removed from DICOM headers using automated deidentification tools, in compliance with HIPAA (Health Insurance Portability and Accountability Act) Safe Harbor guidelines and Article 89 of the GDPR. Each image and clinical record was assigned a unique pseudonymous identifier. Clinical metadata were mapped to standard FHIR R4 resources (Patient, Encounter, Observation, DiagnosticReport, and Consent) using LOINC (Logical Observation Identifiers Names and Codes) and SNOMED CT (Systematized Nomenclature of Medicine–Clinical Terms) terminology mappings. Each data object was tokenized using a cryptographic hash; hash references and minimal governance metadata were stored on the blockchain, while payloads remained encrypted within the IPFS layer. Patients were provisioned with BioWallets containing DIDs and VCs, enabling dynamic and revocable access grants.

Prototype Implementation

The functional prototype was developed in an isolated cloud environment emulating the IT infrastructure of a midsized university hospital. The implementation stack comprised a HAPI FHIR server (Smile Digital Health); Hyperledger Besu with Solidity smart contracts; a Flutter-based BioWallet application integrated with MetaMask and uPort libraries (Consensys); and IPFS with client-side AES-256 encryption. Smart contracts underwent automated static analysis and security scanning using Slither (version 0.10) and Mythril (version 0.24), which identified 0 high-severity vulnerabilities (2 low-severity gas-optimization warnings were resolved prior to deployment), and integration testing confirmed a seamless workflow across FHIR data ingestion, consent management, off-chain governance, and BioWallet-mediated data retrieval.

Evaluation Plan

The prototype was evaluated through a controlled simulation of ICU workflows. Five health care professionals participated (1 senior intensivist, 2 resident physicians, and 2 ICU nurses), each assigned synthetic patient cases under realistic time constraints. This sample was purposively selected to achieve role diversity within the DSR demonstration phase and is explicitly acknowledged as preliminary and exploratory; no inferential statistical analysis is claimed from usability scores. A larger, multisite usability study (20-30 participants) with a validated instrument and a formal interrater reliability assessment is planned as future work.

The baseline latency figure of 125.4 (SD 18.3) seconds was derived from a structured time-and-motion observation at Hospital de Santa Maria (Centro Hospitalar Universitário Lisboa Norte) covering 30 routine EHR/PACS access events during the 4 weeks prior to prototype deployment. Each event was timed from clinician-initiated retrieval to on-screen availability of diagnostic images and metadata. This baseline reflects the specific institutional workflow and may not generalize to other hospital environments.

Smart contract execution time was measured over 50 trials under single-user conditions. Synthetic load testing was performed using Hyperledger Caliper at 10, 25, 50, and 100 concurrent transaction requests (Table 1). A formal STRIDE threat modeling exercise was conducted across all system layers. Security claims are understood to demonstrate that the architecture enforces its intended access control policy under controlled conditions; independent penetration testing is a prerequisite for clinical deployment.

Table 1. Hyperledger Besu throughput and latency under a simulated concurrent load (Hyperledger Caliper benchmark)[a].

Concurrent request	Throughput (TPS[b])	Mean latency (s), (SD)
1	12	1.73 (0.31)
10	41	2.1 (0.35)
25	68	2.6 (0.42)
50	87	3.1 (0.40)
100	94	4.8 (0.61)

[a]The 1-concurrent–request row reflects the same single-user, smart-contract consent-verification measurement reported in evaluation plan and performance outcomes (mean 1.73, SD 0.31; over 50 trials): a Caliper load level of 1 concurrent request is, by construction, the single-user condition, so the 2 figures are not independent measurements.
[b]TPS: transactions per second

Threat Modeling

The framework was designed using a defense-in-depth security model integrating cryptographic controls, decentralized identity mechanisms, smart contract enforcement, and off-chain storage to mitigate both technical and regulatory risks [8,26]. A formal STRIDE threat modeling exercise was conducted across all system components (Table 2).

Table 2. STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege) threat analysis across system components.

Threat	Component	Description	Mitigation	Residual risk
Spoofing	BioWallet/DID[a]	Impersonation via stolen credentials	Biometric authentication+VC[b] expiry	Low
Tampering	IPFS[c]	Modification of off-chain payloads	AES[d]-256 encryption+on-chain hash verification	Low
Repudiation	Smart contract	Denial of access events	Immutable on-chain audit log with timestamps	Very low
Information disclosure	FHIR[e] server	Unauthorized data retrieval	RBAC[f]+off-chain policy evaluation	Low-medium
Denial of service	Blockchain nodes	Node flooding/consensus disruption	Permissioned validator set	Medium
Privilege escalation	Governance layer	Scope escalation via manipulated VC	Policy engine validates scope claims	Low

[a]DID: decentralized identifier.
[b]VC: verifiable credential.
[c]IPFS: InterPlanetary File System.
[d]AES: Advanced Encryption Standard.
[e]FHIR: Fast Healthcare Interoperability Resources.
[f]RBAC: role-based access control.

Ethical Considerations

This study used pseudonymized secondary clinical and imaging data in a simulated ICU environment. Ethical approval was granted by the Ethics Committee of the Hospital de Santa Maria (Centro Hospitalar Universitário Lisboa Norte), approval reference CHULN-EC-2023-047. The legal basis for processing pseudonymized secondary data is grounded in Articles 6(1)(e) and 9(2)(j) of the GDPR, which permit the scientific use of health data in compliance with the principles of lawful processing, data minimization, and purpose limitation. Identifiable patient data are never recorded on-chain; only cryptographic hashes and minimal governance metadata are stored. Informed consent was waived by the ethics committee due to the exclusive use of pseudonymized secondary data processed under the legal bases described above, with reidentification keys retained solely by the approving institution. The participation of the 5 health care professionals in the simulation and usability questionnaire, and the time-and-motion observation of the 30 clinical access events, were covered under approval reference CHULN-EC-2023-047, with data handled and reported anonymously in accordance with the approved ethical protocol. Verbal informed consent was obtained from each of the 5 participating health care professionals prior to their participation in the simulation and usability questionnaire. All procedures comply with the Declaration of Helsinki.

Results

Validation Scenario

The validation simulated an emergency ICU workflow in which a physician, without prior access to institutional records, needed to immediately retrieve chest radiographs and associated clinical metadata to support urgent treatment decisions for a patient with COVID-19–induced ARDS. The scenario covered the full end-to-end process: patient-mediated consent via the BioWallet, blockchain-based access control, FHIR-based data retrieval, and off-chain delivery of encrypted DICOM images. All interactions were mediated through the BioWallet, which enabled visualization of access requests, patient-centric consent authorization, and secure data vault access.

Performance Outcomes

The average elapsed time from BioWallet authentication to successful retrieval and visualization of radiological images and associated clinical metadata was 41.2 (SD 5.6) seconds, corresponding to a 67% reduction relative to the institutional baseline of 125.4 (SD 18.3) seconds. Smart contract-based consent verification averaged 1.73 (SD 0.31, 95% CI 1.64-1.82) seconds over 50 trials. Under concurrent access conditions (Hyperledger Caliper load test at 10 concurrent requests), mean latency increased by approximately 21.4% relative to the single-user baseline (from 1.73 s to 2.10 s; Table 1); full load-test results across 10, 25, 50, and 100 concurrent requests are reported in Table 1. All 5 simulated unauthorized access attempts were blocked (100% prevention rate), and all 25 authorized transactions were immutably recorded with complete traceability of user identifiers, timestamps, request metadata, and data access scopes (Table 3).

Table 3. Key quantitative metrics observed during prototype validation in a simulated intensive care unit (ICU) environment[a].

Metric	Baseline (traditional EHR[b]/PACS[c])	Prototype	Outcome
Average data access latency (s), mean (SD)	125.4 (18.3)	41.2 (5.6)	67% reduction
Smart contract execution (consent)	Not independently measured in this study	1.73 s	Not applicable (no baseline)
Latency increase under concurrent load	N/A[d] (not measured in baseline)	21.4% (10 concurrent requests)	Not applicable (no baseline)
Simulated unauthorized access attempts blocked	Not independently measured	5/5	100% prevention
Authorized transactions correctly audited	Not independently measured	25/25	Full traceability
Ease of use (Likert 1-5)	Not independently measured	4.6	Mean score 4.6/5 (n=5, exploratory)
Perceived security (Likert 1-5)	Not independently measured	4.8	Mean score 4.8/5 (n=5, exploratory)
Preference over existing systems (Likert 1-5)	N/A	4.4	Mean score 4.4/5 (n=5, exploratory)

[a]The institutional data-access latency baseline (125.4 s) was measured directly via the time-and-motion observation described in the evaluation plan. Concurrency degradation was not assessed under the traditional workflow and is therefore reported as not applicable. Baseline values for manual consent-processing time and Likert-scale ease-of-use/security ratings are not reported in this table, as no published source that reported these specific comparator figures under directly comparable conditions was identified; only the prototype values are shown for these 3 metrics.
[b]EHR: electronic health record.
[c]PACS: picture archiving and communication systems.
[d]N/A: not applicable.

Usability and Clinical Acceptability

Usability was assessed using a structured 5-point Likert-scale questionnaire administered to the 5 simulation participants immediately following the evaluation. Mean scores were 4.6 for ease of use, 4.8 for perceived security, and 4.4 for preference over existing institutional systems. These findings are reported as preliminary and exploratory indicators within the DSR demonstration phase only. With n=5, no inferential statistical analysis is appropriate, and the results do not have generalizable validity. Qualitative feedback highlighted the clarity of the consent management interface, the structured presentation of access requests, and the perceived value of patient-mediated access control in time-critical emergency scenarios.

Evaluation of the Governance Function

As defined in the Equation 1, the governance decision function $G(o)$ was exercised over 30 transactions (25 authorized and 5 rejected), with each predicate logged and operating as specified:

- DID resolution and biometric match, $V_{id}(o)$: passed in 25 out of 25 authorized cases and failed in 3 out of 5 rejected cases.
- Policy compliance, $V_{pol}(o)$: failed in 2 out of 5 rejected cases (scope escalation and expired VC).
- Authorization proof, $V_{auth}(o)$: passed in all 25 authorized cases.
- Cryptographic commitment integrity, $C_{hash}(o)$: passed in all 30 cases.

These results confirm that the 4 predicates were logged and operated as specified across the evaluated scenarios. Independent negative testing was observed for the identity and policy predicates, which failed in the corresponding rejected cases; the cryptographic-commitment (integrity) predicate passed in all 30 evaluated cases and was not exercised under failure conditions within this dataset, and its behavior under a failing input remains to be independently verified. Among the rejection cases in which a predicate failure was recorded, the off-chain evaluation order correctly short-circuited on the first failed predicate, minimizing unnecessary computation.

Simulated Attack Scenarios

Five predefined attack scenarios were injected into the simulation: (1) credential misuse by an out-of-scope clinician; (2) invalid digital signature submission; (3) unauthorized scope escalation; (4) replay attack using an expired VC; and (5) unauthenticated direct FHIR end point access. All 5 were successfully blocked, 3 at the off-chain governance layer and 2 at the smart contract enforcement layer. Security claims should be understood as demonstrating that the architecture enforces its intended access control policy only under controlled conditions. Independent third-party penetration testing is a prerequisite for any clinical deployment.

Credential Revocation and DID Resolution Failure

For credential revocation, a previously issued VC was revoked mid-session. The governance layer correctly rejected the subsequent access request within 0.8 seconds of revocation propagation, confirming near-real-time enforcement. For DID resolution failure, the DID resolver was intentionally taken offline during an active session. The system returned an authorization denial and logged the event immutably, with no data exposed. Recovery time after resolver restoration averaged 4.2 seconds.

Residual Risks

Residual risks include the absence of independent penetration testing; the potential for advanced adversarial attacks not covered by predefined scenarios; dependence on DIDComm channel integrity; and the need for adversarial validation in live hospital networks. These are acknowledged as conditions to be met before clinical deployment rather than postdeployment limitations.

Discussion

Principal Findings

The results indicate that the patient-centric architecture integrating FHIR, permissioned blockchain, DIDs, VCs, BioWallets, and off-chain identity-centric governance can substantially reduce data access latency while enhancing security, auditability, and patient autonomy in intensive care environments. The observed 67% latency reduction, combined with 100% prevention of unauthorized access under controlled conditions, suggests that the approach is technically feasible and operationally relevant for time-critical clinical workflows.

Comparison With Prior Work

Compared with prior studies demonstrating blockchain-FHIR integration in oncology, EHR sharing, and clinical research [8,9,19,23], this study extends the literature by incorporating longitudinal medical imaging data, patient-controlled BioWallets, and a validation scenario specifically designed for ICU settings. The integration of the identity-centric governance model [[10]] differentiates the proposed approach from ledger-centric architectures by shifting decision logic to an off-chain control plane supported by VCs and explicit policy rules.

Table 4 summarizes these differences relative to 2 representative blockchain-FHIR systems, FHIRChain [19] and HealthChain [23].

Table 4. Qualitative comparison with FHIRChain and HealthChain across governance, identity, imaging support, consent revocation, and evaluation depth, based on the architectures reported in the cited publications rather than on independent rebenchmarking.

Dimension	FHIRChain [19]	HealthChain [23]	Proposed framework
Governance execution	On-chain smart-contract logic coupled to FHIR[a] pointers	Patient-centered access rules executed on-chain	Off-chain identity/policy evaluation; only commitments and decisions anchored on-chain
Identity model	PKI[b]-based digital certificates	Blockchain account addresses	DIDs[c] and VCs[d]
Imaging support	Not addressed (structured clinical data pointers)	Not addressed (EHR records)	DICOM[e] chest radiographs via encrypted IPFS[f] storage
Consent revocation	Not explicitly modeled	Patient-initiated permission changes	Real-time VC revocation with subsecond enforcement (see *Credential Revocation and DID Resolution Failure*)
Evaluation setting	Conceptual/architectural	Conceptual/architectural with limited benchmarking	Prototype with quantitative latency, load, and simulated-attack evaluation

[a]FHIR: Fast Healthcare Interoperability Resources.
[b]PKI: public key infrastructure.
[c]DID: decentralized identifiers.
[d]VC: verifiable credential.

[e]DICOM: Digital Imaging and Communications in Medicine.
[f]IPFS: InterPlanetary File System.

The adoption of the governance anchor concept has 3 central implications. First, it reduces the data exposure surface by moving identities, clinical artifacts, and semantic evaluation off-chain. Second, it enhances institutional evolvability, as governance rules can be updated at the policy layer without redesigning the ledger. Third, it establishes a feasible pathway for federated interoperability across hospitals and research networks, as governance depends on verifiable predicates rather than homogeneous consensus among all participants.

The dataset of 110 patients and 220 radiographs from a single simulated environment is appropriate for a DSR proof-of-concept, where the objective is to demonstrate artifact functionality rather than establish population-level efficacy [24,25]. Scalability was partially assessed via Caliper load testing (Table 1) but has not been validated at real hospital transaction volumes. Generalizability cannot be claimed from a single-site, single-country simulation. Multicenter pilots across at least 2 jurisdictions, using datasets of ≥500 patients, are planned.

Limitations

This study has several limitations. The evaluation was conducted in a simulated environment rather than in real clinical practice, limiting immediate generalizability. The simulation cohort was small (n=5), and Likert-scale scores are exploratory only. Scalability under larger institutional scenarios was not assessed longitudinally. The implementation has not undergone independent penetration testing or adversarial evaluation in a live hospital network, and the stakeholder sample is Portugal-centric, requiring cross-national validation.

Future Work

Future work should include prospective pilot studies in real ICU settings; integration of real-time ventilatory telemetry; multicenter interoperability assessment; independent penetration testing as a prerequisite for clinical deployment; incorporation of zero-knowledge proofs for enhanced privacy; experimental validation of the identity-centric governance model at scale; and a formal usability study using the System Usability Scale with a minimum of 20 to 30 participants.

Conclusions

This study proposed and evaluated a patient-centric framework integrating FHIR, Hyperledger Besu, IPFS, and a BioWallet, along with an identity-centric governance model, for the management of clinical and imaging data in ICU environments. The evaluation demonstrated the technical feasibility of the artifact within a controlled, single-site proof-of-concept setting. Access latency was reduced by 67% (from 125.4 s to 41.2 s), smart contract consent verification averaged 1.73 (SD 0.31) seconds, all simulated access control violations were blocked, and the identity-centric governance function was logged and operated as specified across all 30 evaluated transactions.

The findings support the view that decoupling governance logic from ledger execution is a technically viable and privacy-preserving approach for regulated health care environments. These conclusions are bounded by the evaluation constraints: a small user cohort (n=5), a single institutional baseline, controlled attack scenarios, and a single-country dataset. Broader claims regarding scalability or widespread adoption are reserved for future multicenter validation.

The proposed framework provides a solid foundation for patient-centric, GDPR-compliant governance of ICU health data, offering a pathway toward federated, privacy-preserving interoperability across institutional and jurisdictional boundaries.

Acknowledgments

The authors gratefully acknowledge the institutional and technical support provided by their affiliated institutions, including the Graduate Program in Computer Science at the Federal University of Pará (UFPA), Molde University College, ISCTE-IUL, and INOV INESC, which contributed to the development and validation of this research.

Generative AI tools, specifically Google Gemini (Pro tier) and OpenAI ChatGPT (Pro tier), were used during the preparation of this manuscript for structural review of the draft text, for spelling and grammar checking throughout the manuscript, and for adjustments to earlier drafts of the figures. In accordance with JMIR policy, representative examples of the prompts and interactions associated with this use are provided in Multimedia Appendix 1. The authors did not retain the original session logs from these tools; therefore, Multimedia Appendix 1 explicitly identifies this material as reconstructed, representative examples rather than verbatim transcripts of the original interactions. All scientific content, data, results, interpretations, conclusions, and conceptual contributions are the exclusive work of the human authors. No AI tool was used to generate, fabricate, or alter research data, figures, references, or scientific claims. The authors take full responsibility for the integrity of the work. AI-assisted illustration tools were used in the preparation of earlier drafts of Figures 1 and 3. Figure 3 has been corrected in the current revision by Claude (Sonnet 5, Anthropic), which edited the original figure image to remove an erroneous embedded text label left over from the earlier AI-assisted draft, leaving the original artwork and layout otherwise unchanged; the corrected figure was reviewed and approved by the authors, who take full responsibility for its accuracy. In accordance with JMIR policy, the instruction used to correct Figure 3 is provided in Multimedia Appendix 1. Figure 1

(PRISMA flow diagram) was also produced with the assistance of the same generative AI tools (Google Gemini [Pro tier] and OpenAI ChatGPT [Pro tier]) used for the earlier figure drafts described above; a representative example of the prompt used is provided in Multimedia Appendix 1. The authors reviewed Figure 1 against the underlying PRISMA counts reported in the Literature Review and confirmed that it is accurate. No other figure in the manuscript was generated or modified using a generative AI tool; Figure 2 (sequence diagram) was created directly by the authors using standard diagramming software. Accordingly, no additional multimedia appendix is required for figure generation beyond Multimedia Appendix 1, which documents the Figure 3 correction and the Figure 1 prompt as described above.

Funding

This work was partially supported by the Brazilian National Council for Scientific and Technological Development (CNPq) under grant numbers 444978/2024-0, 403539/2020-0, and 400111/2023-3; by the Coordination for the Improvement of Higher Education Personnel (CAPES), Brazil; by the São Paulo Research Foundation (FAPESP) under grant numbers 2023/00811-0, 2023/00673-7, 2021/00199-8 (CPE SMARTNESS), 2020/04031-1, and 2018/23097-3; and by the Telecommunications Research and Development Center (CPqD). No funding was received from the journal, the publisher, or any party with a financial interest in the results of this research.

Data Availability

The dataset used in this study was pseudonymized prior to processing, in compliance with Article 89 of the GDPR; reidentification keys are held solely by the approving institution and were not accessible to the research team. Public availability of the data will be determined in accordance with applicable ethical guidelines and institutional policies. Code and test scripts will be made available upon request.

Authors' Contributions

EBEC, JCAF, and AJGA contributed to the conceptualization of the study. EBEC and JCAF designed the methodology. EBEC developed the software (prototype implementation, smart contracts, and the BioWallet application), performed the formal analysis, and conducted the investigation, including data curation and validation experiments. JCAF and AJGA supervised the research, provided resources, and acquired funding. EBEC wrote the original draft; JCAF and AJGA reviewed and edited the manuscript. EBEC prepared the visualizations. All authors have read and approved the final manuscript and confirm that they meet the authorship criteria.

Conflicts of Interest

None declared.

Multimedia Appendix 1

Generative AI use during manuscript preparation—prompt documentation.
[DOCX File (Microsoft Word File), 523 KB-Multimedia Appendix 1]

References

1. Noteboom SH, Kho E, Galanty M, et al. From intensive care monitors to cloud environments: a structured data pipeline for advanced clinical decision support. EBioMedicine. Jan 2025;111:105529. [doi: 10.1016/j.ebiom.2024.105529] [Medline: 39731854]
2. da Silva AA, Merolli M, Fini NA, Granger CL, Gustafson OD, Parry SM. Digital health interventions in adult intensive care and recovery after critical illness to promote survivorship care. J Intensive Care Soc. Feb 2025;26(1):96-104. [doi: 10.1177/17511437241311105] [Medline: 39764433]
3. Negro-Calduch E, Azzopardi-Muscat N, Krishnamurthy RS, Novillo-Ortiz D. Technological progress in electronic health record system optimization: systematic review of systematic literature reviews. Int J Med Inform. Aug 2021;152:104507. [doi: 10.1016/j.ijmedinf.2021.104507] [Medline: 34049051]
4. Leonard J, Sinha P. Precision medicine in acute respiratory distress syndrome: progress, challenges, and the road ahead. Clin Chest Med. Dec 2024;45(4):835-848. [doi: 10.1016/j.ccm.2024.08.005] [Medline: 39443001]
5. Khader F, Müller-Franzes G, Wang T, et al. Multimodal deep learning for integrating chest radiographs and clinical parameters: a case for transformers. Radiology. Oct 2023;309(1):e230806. [doi: 10.1148/radiol.230806] [Medline: 37787671]
6. Li E, Clarke J, Ashrafian H, Darzi A, Neves AL. The impact of electronic health record interoperability on safety and quality of care in high-income countries: systematic review. J Med Internet Res. Sep 15, 2022;24(9):e38144. [doi: 10.2196/38144] [Medline: 36107486]
7. Heumos L, Ehmele P, Treis T, et al. An open-source framework for end-to-end analysis of electronic health record data. Nat Med. Nov 2024;30(11):3369-3380. [doi: 10.1038/s41591-024-03214-0] [Medline: 39266748]
8. Gordon WJ, Catalini C. Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability. Comput Struct Biotechnol J. 2018;16:224-230. [doi: 10.1016/j.csbj.2018.06.003] [Medline: 30069284]

9. Dubovitskaya A, Baig F, Xu Z, et al. ACTION-EHR: patient-centric blockchain-based electronic health record data management for cancer care. J Med Internet Res. Aug 21, 2020;22(8):e13598. [doi: 10.2196/13598] [Medline: 32821064]
10. Faber B, Michelet GC, Weidmann N, Mukkamala RR, Vatrapu R. BPDIMS:a blockchain-based personal data and identity management system. 52nd Hawaii Int Conf Syst Sci. Jan 8, 2019:6855-6864. [doi: 10.24251/HICSS.2019.821]
11. Page MJ, McKenzie JE, Bossuyt PM, et al. The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. BMJ. Mar 29, 2021;372:n71. [doi: 10.1136/bmj.n71] [Medline: 33782057]
12. Amar F, April A, Abran A. Electronic health record and semantic issues using Fast Healthcare Interoperability Resources: systematic mapping review. J Med Internet Res. Jan 30, 2024;26:e45209. [doi: 10.2196/45209] [Medline: 38289660]
13. Vorisek CN, Lehne M, Klopfenstein SAI, et al. Fast Healthcare Interoperability Resources (FHIR) for interoperability in health research: systematic review. JMIR Med Inform. Jul 19, 2022;10(7):e35724. [doi: 10.2196/35724] [Medline: 35852842]
14. Nguyen TA. Digital Twin, Blockchain, and Sensor Networks in the Healthy and Mobile City. 1st ed ed. Elsevier; 2025. ISBN: 978-0-443-34174-8
15. Sahoo A, Sobhanayak S. EBH-IoT: energy-efficient secured data collection and distribution of electronics health record for cloud assisted blockchain enabled IoT based healthcare system. J Ind Inf Integr. Nov 2024;42:100702. [doi: 10.1016/j.jii.2024.100702]
16. Razavian SB, Tirkolaee EB, Simic V, Ali SS, Görçün ÖF. Blockchain-enabled healthcare supply chain management: identification and analysis of barriers and solutions based on improved zero-sum hesitant fuzzy game theory. Eng Appl Artif Intell. Aug 2025;154:110991. [doi: 10.1016/j.engappai.2025.110991]
17. Benchoufi M, Altman D, Ravaud P. From clinical trials to highly trustable clinical trials: blockchain in clinical trials, a game changer for improving transparency? Front Blockchain. 2019;2:23. [doi: 10.3389/fbloc.2019.00023]
18. Holmes JH, Beinlich J, Boland MR, et al. Why is the electronic health record so challenging for research and clinical care? Methods Inf Med. May 2021;60(1-02):32-48. [doi: 10.1055/s-0041-1731784] [Medline: 34282602]
19. Zhang P, White J, Schmidt DC, Lenz G, Rosenbloom ST. FHIRChain: applying blockchain to securely and scalably share clinical data. Comput Struct Biotechnol J. 2018;16:267-278. [doi: 10.1016/j.csbj.2018.07.004] [Medline: 30108685]
20. Tahir NUA, Rashid U, Hadi HJ, et al. Blockchain-based healthcare records management framework: enhancing security, privacy, and interoperability. Technologies (Basel). 2024;12(9):168. [doi: 10.3390/technologies12090168]
21. Gazzarata R, Almeida J, Lindsköld L, et al. HL7 Fast Healthcare Interoperability Resources (HL7 FHIR) in digital healthcare ecosystems for chronic disease management: scoping review. Int J Med Inform. Sep 2024;189:105507. [doi: 10.1016/j.ijmedinf.2024.105507] [Medline: 38870885]
22. Dai H, Young HP, Durant TJS, et al. TrialChain: a blockchain-based platform to validate data integrity in large, biomedical research studies. arXiv. Preprint posted online on Jul 10, 2018. [doi: 10.48550/arXiv.1807.03662]
23. Hylock RH, Zeng X. A blockchain framework for patient-centered health records and exchange (HealthChain): evaluation and proof-of-concept study. J Med Internet Res. Aug 31, 2019;21(8):e13592. [doi: 10.2196/13592] [Medline: 31471959]
24. Hevner AR, March ST, Park J, Ram S. Design science in information systems research. MIS Q. Mar 1, 2004;28(1):75-106. [doi: 10.2307/25148625]
25. Peffers K, Tuunanen T, Rothenberger MA, Chatterjee S. A design science research methodology for information systems research. J Manag Inf Syst. Dec 2007;24(3):45-77. [doi: 10.2753/MIS0742-1222240302]
26. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). European Union; Apr 2016. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng [Accessed 2026-09-16]

Abbreviations

ACM: Association for Computing Machinery
AES: Advanced Encryption Standard
ARDS: acute respiratory distress syndrome
DICOM: Digital Imaging and Communications in Medicine
DID: decentralized identifier
DSR: design science research
EHR: electronic health record
FHIR: Fast Healthcare Interoperability Resources

GDPR: General Data Protection Regulation
HIPAA: Health Insurance Portability and Accountability Act
ICU: intensive care unit
IPFS: InterPlanetary File System
LOINC: Logical Observation Identifiers Names and Codes
PACS: picture archiving and communication system
PRISMA: Preferred Reporting Items for Systematic Reviews and Meta-Analyses
SNOMED CT: Systematized Nomenclature of Medicine–Clinical Terms
STRIDE: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege
VC: verifiable credential

Edited by Mamdooh Alzyood; peer-reviewed by Allan Silva Freitas, Bright Keswani, Diego de Abreu, Niranjan Lal; submitted 21.Apr.2026; initial comments to author 23.Jun.2026; final revised version received 05.Aug.2026; accepted 06.Aug.2026; published 25.Nov.2026

Please cite as:
Evaristo Correa Sr EB, Amaro Ferreira Sr 2nd JC, Gomes Abelém Sr 3rd AJ
Identity-Centric Blockchain Framework for Medical Imaging Data Governance in Intensive Care Unit Patients With COVID-19–Associated Acute Respiratory Distress Syndrome: Development and Usability Study
JMIR Form Res 2026;10:e99002
URL: https://formative.jmir.org/2026/1/e99002
doi: 10.2196/99002

© Elder Bruno Evaristo Correa Sr, João Carlos Amaro Ferreira Sr 2nd, Antonio Jorge Gomes Abelém Sr 3rd. Originally published in JMIR Formative Research (https://formative.jmir.org), 25.Nov.2026. This is an open-access article distributed under the terms of the Creative Commons Attribution License (https://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work, first published in JMIR Formative Research, is properly cited. The complete bibliographic information, a link to the original publication on https://formative.jmir.org, as well as this copyright and license information must be included.