

Blockchain-enabled secure and patient-centric genomic data management: a governance framework

Poonam Gangwar¹, Raj K. Keservani^{2,*}, Anuj Nautiyal¹, Rahul Roy¹, Rohit Kumar Kesharwani³, Abhijeet Ojha⁴

¹ School of Pharmaceutical Sciences, Shri Guru Ram Rai University, Patel Nagar, Dehradun-248001, Uttarakhand, India

² Laboratory of Pharmaceutics, Faculty of B. Pharmacy, CSM Group of Institutions, Prayagraj, Uttar Pradesh, 212111, India

³ Madhu Vachaspati Institute of Pharmacy (Affiliated to Dr. APJ Abdul Kalam Technical University, Lucknow), Puramufti Kaushambi, Uttar Pradesh, 212213, India

⁴ Faculty of Pharmaceutical Sciences, Amrapali University, Haldwani, Uttarakhand, India

* Correspondence: rajksops@gmail.com

ABSTRACT

The rapid growth of genomic data is essential for advancing personalised medicine. However, it is hindered by vulnerabilities in current centralised management systems, such as privacy breaches, opaque data usage, and limited individual control. These issues undermine public trust and slow ethical progress in precision healthcare. This chapter critically explores how blockchain technology, owing to its decentralisation, immutability, and cryptographic security, offers a transformative framework for genomic data governance. It focuses on blockchain-based systems that enable secure, patient-centred data management. It discusses mechanisms like smart contracts for detailed access control, hybrid on/off-chain storage solutions for handling large datasets, and immutable audit trails to ensure transparency and compliance. Additionally, the chapter examines key challenges in implementation, including alignment with regulations like GDPR and HIPAA, interoperability with existing biomedical standards, and balancing data permanence with ethical rights such as data erasure. By combining technical design with governance principles, this work presents a multidisciplinary framework that positions blockchain as a fundamental technology for secure, transparent, and fair genomic data management, promoting the responsible realisation of personalised medicine's potential.

Submitted: 12 August 2026

Revised: 09 September 2026

Accepted: 16 September 2026

Published: 29 September 2026

ISSN: 2449-8955

Copyright: © 2026 The Author(s).

Published by JBródka Publisher.

This is an open access article

under the [CC BY 4.0 license](#).

Publisher's Note: The opinions and statements in this publication are solely those of the Authors and do not represent JBródka Publisher or the editors, who disclaim responsibility for any consequences arising from the use of the presented information.

KEYWORDS: Blockchain; Genomic; Computation; HIPAA/GDPR; FAIR; Biomedical informatics

DOI: <http://dx.doi.org/10.5281/zenodo.23045506>

INTRODUCTION

The integration of genomic data into healthcare and research stands as a cornerstone of precision medicine, promising unprecedented advancements in disease prediction, diagnosis, and tailored therapeutics. However, the very value of this sensitive data is undermined by profound systemic vulnerabilities in its management. Traditional genomic data systems, typically reliant on centralised or siloed repositories, are increasingly inadequate for modern demands. They present critical single points of failure, are prone to security breaches and unauthorised secondary use, and often lack transparent mechanisms for patient consent and data provenance. This architecture fails to guarantee true data ownership for individuals, creating inequities and eroding the trust essential for widespread participation in genomic research [1]. Furthermore, existing frameworks struggle with interoperability, hindering collaborative science, and are often misaligned with evolving data protection regulations such as the GDPR and HIPAA, particularly concerning rights to data erasure and granular consent [2]. This confluence of technical, ethical, and regulatory shortcomings constitutes a

significant research gap: the need for a governance-aware technological framework that can simultaneously ensure security, auditability, and individual sovereignty over genomic information.

Blockchain (Fig. 1) technology emerges as a transformative alternative to these conventional paradigms. Characterised by its decentralised ledger, cryptographic immutability, and programmable smart contracts, blockchain offers a foundational shift toward secure and patient-centric data governance. It enables the creation of tamper-evident audit trails for all data access and usage, provides a mechanism for executing dynamic consent agreements via code, and facilitates patient control through decentralised digital identities. By design, it mitigates risks associated with central authority control and opaque data handling [3]. In genomic applications, blockchain is not merely a storage solution but a regulatory and ethical technology layer that can authenticate data integrity, manage access permissions, and ensure compliance in a transparent manner [4]. This chapter, therefore, investigates the convergence of blockchain and genomic data management. It will critically analyse how blockchain's core properties address the identified deficiencies of traditional systems, explore viable architectural models and their inherent challenges, and synthesise a multidisciplinary framework that aligns technological innovation with robust ethical and regulatory standards to advance the equitable future of genomic medicine [3, 5].

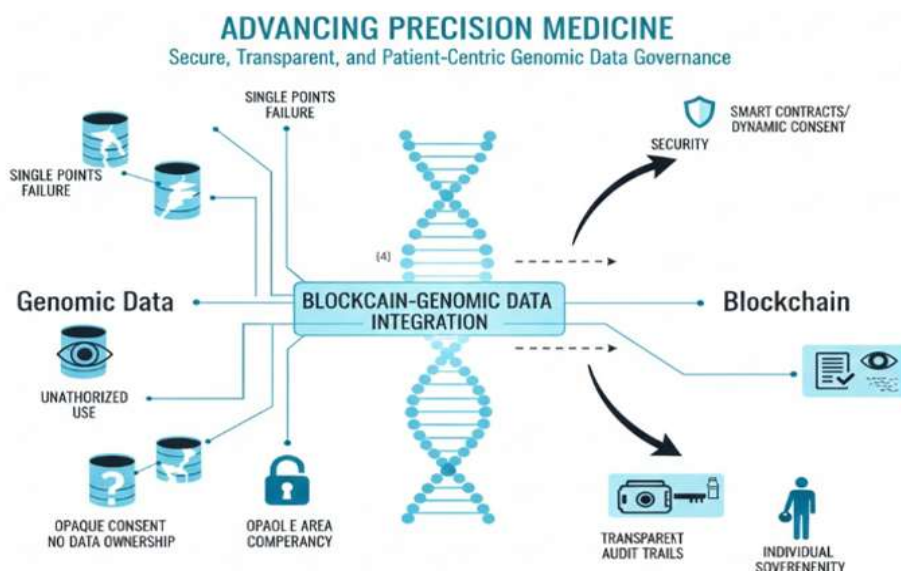


Figure1. Blockchain.

BLOCKCHAIN: PROPERTIES AND LIMITATIONS

CORE PROPERTIES

Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets across a business network. Anything of value can be tracked and traded on the Blockchain network. A Blockchain is a distributed database, which is shared over a computer network. Blockchain stores information electronically in a digital format to make transactions secure [6].

Blockchain is a new technology, which is known as Distributed Ledger Technology (DLT). With the help of Blockchain technology, currency, as well as anything, can be converted into a digital format and stored. Actually, it is an exchange process, which works on data blocks. In this, one block is connected to another block. These blocks cannot be hacked. Blockchain technology aims to keep documents digitally secure. You can take Google Docs as an example to understand Blockchain technology. When we create a document and share it with a group of people, the document is distributed instead of copied or transferred. But, Blockchain is more

complex than Google Docs. Blockchain technology aims to keep records digitally secure through decentralised verification and cryptographic hashing [7].

CRITICAL DISTINCTION: BLOCKCHAIN PROPERTIES VS SYSTEM-LEVEL PROPERTIES

A Fundamental distinction must be made between what blockchain technology itself guarantees and what the entire system must provide block chain ensures:

- Immutability: Once recorded, transactions cannot be altered without network consensus
- Auditability: All transactions are permanently recorded and verifiable
- Cryptographic verification: Digital signatures authenticate participants
- However, blockchain does not automatically ensure:
- Privacy: Transaction visibility may leak information
- Interoperability: Standards must be categorically designed
- Data protection compliance: GDPR rights to ensure conflict with immutability
- Quality of data: Blockchain ensures the integrity of record nor data accuracy

SECURITY LIMITATION AND VULNERABILITIES

Blockchain technology, “cannot be hacked” was a wrong statement and it requires clarification [8]. Potential threat vectors are:

- Key: Compromise private keys, which allows unauthorised transactions
- Code errors: If code gets corrupted, like Re-entrancy attacks
- Infrastructures: If the infrastructure of the work network it not strong enough, then it's a high risk; 51% attacks can be done on the structure of the work network
- Manipulative data: Blockchain cannot filter incorrect data from being recorded
- Advanced searchable encryption: Quantum computing threatens current encryption standards

GENOMIC DATA /GENOMIC DATA MANAGEMENT

CURRENT LANDSCAPE AND CHALLENGES

The effective management of genomic data is a multifaceted challenge that extends beyond mere storage, encompassing its entire lifecycle from generation to clinical application. This process - spanning collection, annotation, sharing, and consent management - is fraught with technical, ethical, and logistical hurdles that undermine its potential. The adoption of global data governance frameworks like the FAIR (Findable, Accessible, Interoperable, Reusable) principles, the Global Alliance for Genomics and Health (GA4GH) standards, and ISO/TC 276 specifications for biotechnology aims to create order. However, their implementation remains inconsistent, exposing systemic gaps that blockchain technology is uniquely positioned to address [9,10].

DATA LIFECYCLE VULNERABILITIES AND GOVERNANCE GAPS

COLLECTION & CONSENT MANAGEMENT (FIG. 2)

The initial stage of data collection is often compromised by insufficient informed consent mechanisms. Traditional models are static and binary, failing to accommodate future, unspecified research uses or allow participants to dynamically withdraw consent - a direct conflict with regulations like the GDPR [11]. Furthermore, the principle of data minimisation is frequently violated, as entire genomes are collected when only specific loci are relevant, unnecessarily amplifying privacy risks [12]. This creates a foundational deficit in trust and ethical compliance.

ANNOTATION & STANDARDISATION

Following collection, genomic data must be annotated with phenotypic and clinical information to be useful. A lack of universal standards at this stage, despite the guidelines provided by GA4GH and ISO/TC 276, leads to heterogeneous formats and ontologies. This heterogeneity cripples interoperability, making data sharing and meta-analysis across institutions and international borders inefficient and error-prone, thereby siloing valuable research insights [13].

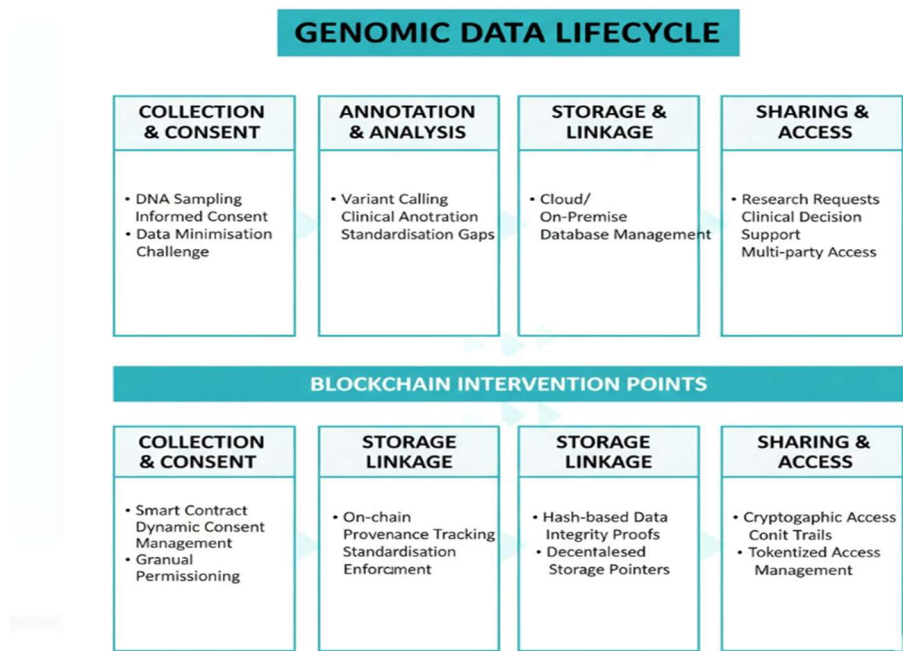


Figure 2. Lifecycle of genomic data.

SHARING & SECURITY

The sharing of genomic data for research or clinical collaboration is hindered by legitimate security concerns. Centralised repositories present attractive targets for cyberattacks, and anonymisation has proven reversible [14]. Simultaneously, researchers face administrative burdens in accessing controlled datasets. This creates a paradox where data is simultaneously insecure and inaccessible, stifling collaboration and slowing scientific progress [15].

ANALYTICAL LINK TO BLOCKCHAIN-BASED SOLUTIONS

The challenges within each stage of the genomic data lifecycle find potential resolution in the core attributes of blockchain technology, creating a direct analytical link between problem and solution.

FROM STATIC TO DYNAMIC CONSENT

Blockchain-enabled smart contracts can transform consent management from a static document into a programmable, dynamic consent framework. Participants can grant, modify, or revoke access permissions for specific data uses in real-time, with every transaction immutably logged. This directly addresses ethical gaps and automates compliance with data subject rights [16,17].

ENHANCING INTEGRITY AND INTEROPERABILITY

Storing cryptographic hashes of genomic datasets (or key annotations) on-chain provides an immutable proof of data integrity and provenance. Furthermore, smart contracts can enforce the use of GA4GH-standardised

formats for data deposition, promoting interoperability by design [18]. Access to data can be contingent on agreement to standardised terms, streamlining sharing (Table 1).

SECURING ACCESS AND AUDITABILITY

Blockchain facilitates a shift from security-through-obscurity to cryptographic access control. Data can remain encrypted in off-chain storage (e.g., decentralised systems like IPFS), while on-chain smart contracts govern the decryption keys. Every data access request and fulfilment is recorded on an immutable ledger, creating a transparent and fully auditable trail that enhances security and builds trust among all stakeholders [19].

Table 1. Enhancing Integrity and Interoperability.

Genomic Data Challenge	Blockchain Solution	Mechanism
Static consent models	Dynamic consent via smart contracts	Programmable, revocable, granular access permissions
Data integrity concerns	Immutable cryptographic hashing	Tamper-evident provenance tracking
Interoperability gaps	Standard-enforcing smart contracts	Automated compliance with GA4GH/FAIR principles
Opaque access control	Cryptographic access logging	Transparent, auditable permission trails
Centralised vulnerability	Decentralised storage+ledger	Eliminated single points of failure

ANALYTICAL LINK: MAPPING CHALLENGES TO BLOCKCHAIN SOLUTIONS

Genomic data is the complete set of an organism's genetic instructions, primarily its DNA sequence, that provides the blueprint for its growth and functioning. It includes the order of chemical building blocks (nucleotides) in an organism's genes, regulatory elements, and the relationships between genes, which are vital for understanding health, disease, and evolution. This data is collected through DNA analysis and used in personalised medicine, helping to develop targeted therapies, predict genetic risks, and diagnose diseases. Genomic Data Management, in its most accessible form, involves organising, storing, and tracking information derived from an organism's genetic makeup. Imagine a vast library holding billions of biological instruction manuals, each for a unique individual.

CHALLENGES IN GEONOMIC DATA MANAGEMENT

Modern medicine, particularly personalised therapies and gene editing, increasingly relies on genomic data that is high-quality, secure, and standardised. However, genomic data management is fraught with challenges, including privacy and security risks, inconsistent regulatory frameworks, logistical complexities, public trust issues, and unresolved ethical concerns. These challenges must be addressed to fully realise the benefits of genomic data while protecting individual rights and fostering trust (Table 2) [20-23].

Table 2. Challenges in genomic data management.

Challenge Category	Specific Issues	Consequences
Privacy & Security	Re-identification risks, DTC data breaches, data oversharing	Identity theft, genetic discrimination, eroded trust
Regulatory Compliance	Conflicts between immutability and “right to be forgotten”, unclear ownership in a decentralised system	Legal vulnerabilities, inhibited adoption
Technical & Logistical	Massive data volumes(100+ GB per genome), lack of standardised formats	High costs, interoperability barriers, and scalability issues
Public Trust & Ethics	Unauthorised data sharing, genetic surveillance, opaque consent process	Reduced participation, biased datasets, and ethical violations

PRIVACY AND SECURITY RISK

Genomic data is uniquely identifiable, containing sensitive information about an individual's ancestry, health risks, and genetic predispositions. Unauthorised access to such data can lead to identity theft, genetic discrimination, and secondary use without informed consent. For instance [14]. Demonstrated how anonymised genomic datasets could be re-identified through surname inference, illustrating significant vulnerabilities in current privacy protections. Furthermore, DTC genomic testing companies, have been criticised for inadequate security measures. Fahs notes that these companies often collect and store raw genomic data without robust encryption, increasing the likelihood of breaches [24,25]. Even more troubling, these companies have faced allegations of selling consumer data to third parties without sufficient transparency, further eroding trust [27]. An equally pressing issue is the problem of data oversharing, where individuals are required to provide their entire genomic sequence even when only a small segment is necessary for research or clinical purposes. This unnecessary exposure amplifies privacy risks, as the full dataset contains sensitive information that can be exploited if accessed improperly. Such practices are not only ethically questionable but also conflict with data minimisation principles emphasised in frameworks like GDPR [11]. These privacy concerns are compounded by cases where DTC companies cooperate with law enforcement. For example, Ancestry has provided customer data to police, leading to the identification and arrest of relatives of their customers. While this has helped solve crimes, it raises ethical questions about informed consent and the potential for misuse of genetic data [29]. Such practices highlight the fine line between public safety and individual privacy, underscoring the need for clearer policies and protections.

REGULATORY COMPLIANCE AND BLOCKCHAIN TENSIONS

Regulatory oversight for blockchain in genomic data management requires careful attention to existing data protection laws. The immutability of blockchain creates inherent tension with GDPR's "right to be forgotten" [26]. While our proposed architecture mitigates this through off-chain data storage, on-chain elements (hashes, CIDs, metadata) may still constitute personal data under GDPR. The challenge lies in designing systems that balance blockchain's permanence with regulatory requirements, potentially through:

- Dynamic consent mechanisms that allow permission revocation without deleting data
- Off-chain storage of identifiable information
- Cryptographic techniques for selective disclosure
- Clear jurisdictional frameworks for cross-border data flows [27].

LOGISTICAL AND TECHNICAL COMPLEXITIES

The massive size of genomic datasets presents significant logistical and technical challenges. A single genome sequence can exceed 100 gigabytes, and with the growth of personalised medicine, data volumes are increasing exponentially [28]. Current storage and computational infrastructures struggle to manage these volumes efficiently, leading to high costs and potential data loss [29]. The lack of standardised data formats complicates collaboration between research institutions and healthcare providers, limiting scalability [30].

PUBLIC TRUST AND PARTICIPATION

Trust in genomic data management is critical for fostering public participation in research. However, trust has been undermined by cases of genetic surveillance and unauthorised data sharing [31]. Consumers are increasingly wary of contributing their genomic data due to fears of misuse, including tracking by governments or corporations for purposes beyond their consent [32]. Such concerns deter participation, reducing dataset diversity and limiting scientific discoveries [33].

ETHICAL CONCERNS AND INFORMED CONSENT

Ethical issues surrounding genomic data include informed consent, data ownership, and equitable access control. Many current consent processes are insufficiently transparent, leaving individuals unaware of how their data will be used, stored, or shared [11]. This lack of clarity undermines autonomy and can lead to unintended consequences, such as data commercialisation without fair compensation [24]. Additionally, genetic discrimination remains a persistent concern, highlighting the need for stronger ethical frameworks [34].

BLOCKCHAIN-BASED GENOMIC DATA ARCHITECTURE

The transformative potential of blockchain for genomic data management is realised through a structured, multi-layered architectural framework. This framework moves beyond theoretical benefits to define a concrete, interoperable system that addresses the full data lifecycle. At its core, it decouples the massive storage of genomic data from the management of its access rights and audit history, leveraging the strengths of both decentralised file systems and permissioned blockchain networks. A proposed architecture, visualised in Figure 3, consists of four integrated layers [31-33].

CRITICAL ASSESSMENT: WHAT BLOCKCHAIN DOES AND DOES NOT GUARANTEE

Before detailing the architecture, it is essential to clarify the capabilities and limitations of blockchain in this context:

- What blockchain contributes:
- Immutable audit trails for access events
- Cryptographic proof of data integrity through hashing
- Decentralised consensus for policy enforcement
- Automated compliance through smart contracts
- Patient-controlled access permissions
- What blockchain cannot guarantee without additional system design:
- Privacy of data (encryption is required)
- Interoperability with existing systems (standards must be adopted)
- GDPR compliance (system design must address this)
- Security against key compromise (key management is critical)
- Data quality or correctness (blockchain records only what is submitted)

MULTI-LAYERED ARCHITECTURE

The architecture consists of four integrated layers (Figure 3):

- Data Ingestion Layer: Client-side encryption and hashing
- Storage Layer: Decentralised or secure off-chain storage
- Blockchain Ledger Layer: Permissioned blockchain with smart contracts
- Access and Audit Layer: API gateway with consent validation

DETAILED DATA FLOW AND TECHNICAL MECHANISMS

Step 1: Secure Data Ingestion and Preparation

The process begins at the Data Ingestion Layer. Prior to upload, raw genomic data (e.g., a FASTQ or VCF file) undergoes client-side encryption (e.g., using AES-256) to ensure confidentiality. Sensitive direct identifiers are pseudonymized. A cryptographic hash (e.g., SHA-256) of the encrypted data is computed, creating a unique, immutable digital fingerprint for integrity verification [37].

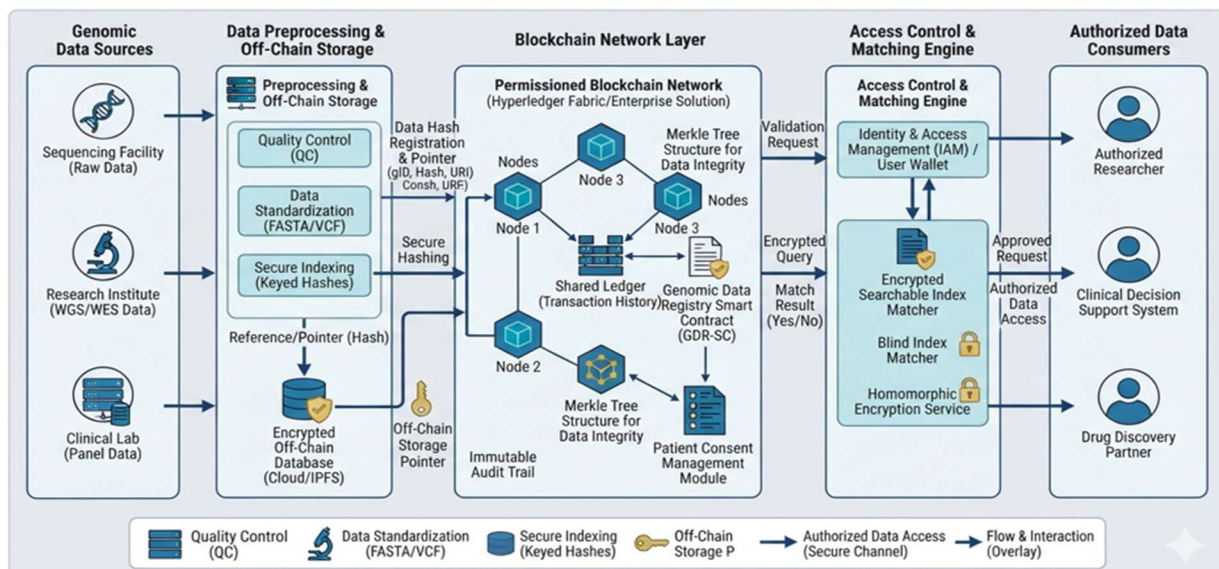


Figure 3. Blockchain-genomic data integration architecture.

Step 2: Off-Chain Storage in Distributed Systems

The encrypted data file is transmitted to the Storage Layer, which may utilize a decentralized file system like the InterPlanetary File System (IPFS) or a secure cloud vault. Critical consideration: IPFS does not inherently ensure confidentiality, access control, or GDPR compliance. Its suitability for genomic data must be justified through:

- Integration with encryption layers
- Permissioned networks (private IPFS)
- Additional access control mechanisms
- Metadata sanitisation before storage

Upon storage, a content-based address (Content Identifier or CID) is generated. The data itself is not stored on the blockchain, ensuring scalability [38].

Step 3: On-Chain Registration and Policy Anchoring

The hash and the storage CID are sent to the Blockchain Ledger Layer as a transaction. A smart contract acts as a regulatory compliance and access gateway, creating a permanent record associating the data hash with its storage location. The data owner defines an access policy within this transaction, encoded into the smart contract's logic [39].

Step 4: Consent-Validated Access and Verification

When a researcher or clinician requires access, they initiate a request through the Access and Audit Layer by submitting a transaction signed with their private key. The relevant smart contract validates the request against the embedded policy and the requester's decentralised identity [40]. If conditions are met, the contract executes, enabling retrieval of the data CID and decryption key.

DECRYPTION KEY MANAGEMENT: CRITICAL SECURITY ELEMENT

A key security consideration is the management of decryption keys. The architecture must specify:

- Key storage: Hardware security modules (HSMs), key management services
- Key recovery: Backup mechanisms, multi-party computation
- Key invalidation: Revocation protocols, key rotation schedules
- Access to keys: Integration with smart contract policies
- Key exchange: Secure channels, distributed key generation

Without addressing these elements, the security of the entire system is compromised [41].

SMART CONTRACTS IN CONSENT AND COMPLIANCE

Smart contracts automate governance through (Figure 4):

- Dynamic Consent Management: Granular, time-bound, revocable permissions
- Automated Compliance: Enforcement of regulatory rules through credential verification
- Audit Trails: Immutable logging of all access events
- Limitation: Smart contracts are only as reliable as their code quality and cannot enforce compliance with regulations like GDPR when contradictions exist [42].

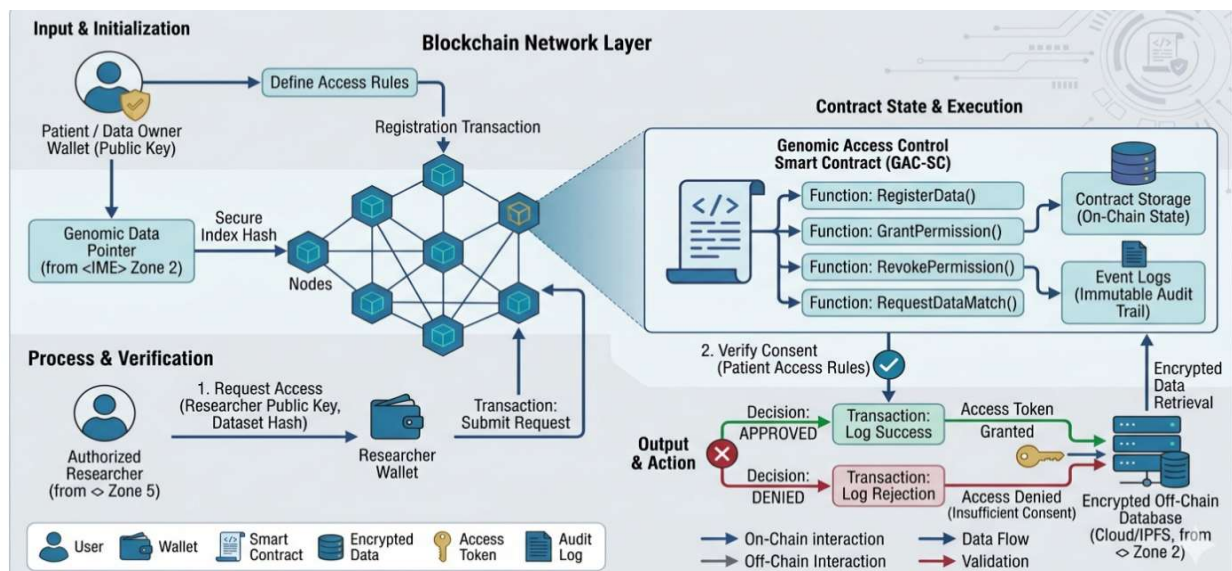
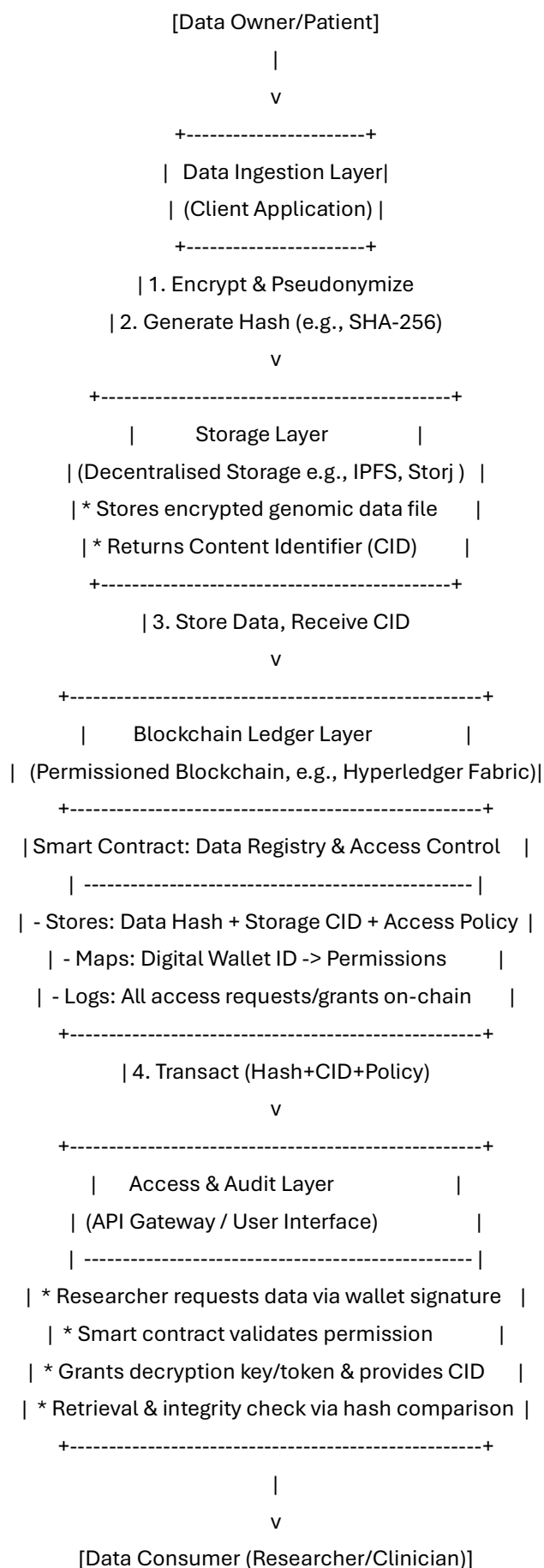


Figure 4. Smart contract-based management.

Blockchain-Genomic Data Integration Architecture





DETAILED DATA FLOW AND TECHNICAL MECHANISMS

Step 1: Secure Data Ingestion & Preparation

The process begins at the Data Ingestion Layer. Prior to upload, raw genomic data (e.g., a FASTQ or VCF file) undergoes client-side encryption (e.g., using AES-256) to ensure confidentiality. Sensitive direct identifiers are pseudonymized. A cryptographic hash (e.g., SHA-256) of the encrypted data is computed, creating a unique, immutable digital fingerprint that will be used for integrity verification.

Step 2: Off-Chain Storage in Distributed Systems

The encrypted data file is transmitted to the Storage Layer, which utilizes a decentralized file system like the InterPlanetary File System (IPFS) or a secure cloud vault. This layer is optimized for handling large-scale data. Upon storage, a content-based address (Content Identifier or CID) is generated, which points to the data's location. The data itself is not stored on the blockchain, ensuring scalability.

Step 3: On-Chain Registration & Policy Anchoring

The hash and the storage CID are sent to the Blockchain Ledger Layer as a transaction. A smart contract - a self-executing program deployed on the blockchain - acts as a regulatory compliance and access gateway. This contract creates a permanent record associating the data hash with its storage location. Crucially, the data owner defines an access policy within this transaction. This policy, encoded into the smart contract's logic, specifies rules such as "Wallet X can read this data for purpose Y until date Z" or "Allow access only if the requester's credential is signed by Institution A."

Step 4: Consent-Validated Access & Verification

When a researcher or clinician (Data Consumer) requires access, they initiate a request through the Access & Audit Layer by submitting a transaction signed with their private key. The relevant smart contract automatically validates the request against the embedded policy and the requester's decentralised identity (linked to their digital wallet). If the conditions are met, the contract executes: it can emit a token or permission message, which the Access Layer uses to retrieve the decryption key (managed via a secure key service) and the data CID from storage. The consumer downloads the encrypted data, decrypts it, and recomputes its hash. By comparing this hash to the immutable hash stored on-chain, they can cryptographically verify the data's integrity and provenance, ensuring it has not been altered [34, 35].

THE ROLE OF SMART CONTRACTS IN CONSENT AND COMPLIANCE

Smart contracts are the operational heart of this architecture, automating governance (Figure 5):

- **Dynamic Consent Management:** They enable granular, time-bound, and revocable consent. An owner can update the smart contract's policy to change permissions, with all changes immutably logged.
- **Automated Compliance:** Contract logic can enforce regulatory rules by checking credentials (e.g., verifying a researcher's IRB approval hash) before granting access, creating a self-enforcing ethical layer.

This architecture provides a blueprint for a system that is simultaneously secure (cryptographically enforced), transparent (fully auditable), scalable (off-chain data storage), and patient-centric (policy-driven access) [36-38].

REGULATORY OVERSIGHT

Regulatory oversight for blockchain in genomic data management requires compliance with existing data protection laws like HIPAA and GDPR, establishing clear frameworks for informed consent and data ownership in decentralised systems, and promoting interoperability standards for seamless integration. Regulations should also mandate robust security measures, establish protocols for breach notifications, and address the

challenges of reconciling blockchain's immutability with patients' right to be forgotten through solutions like dynamic consent and off-chain data storage [43-45].

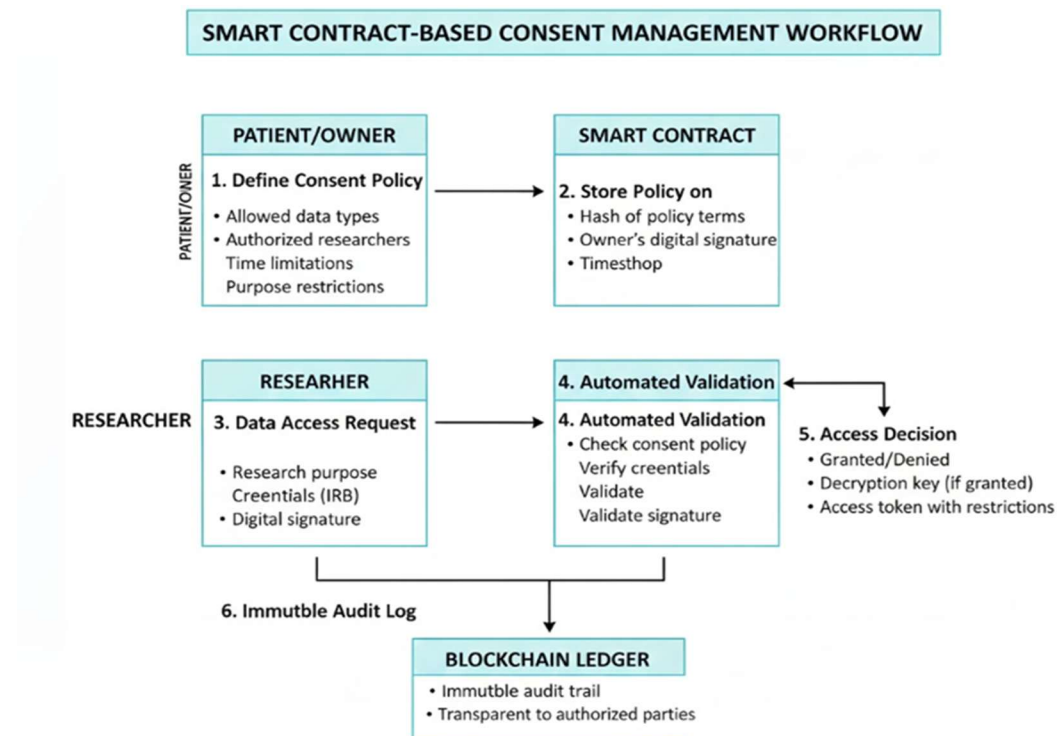


Figure 5. Smart contract-based management.

THREAT MODEL AND ADVERSARIAL SCENARIOS

A rigorous security analysis requires specifying the threat model:

Types of adversaries:

1. External attackers: Steal keys, intercept communications, exploit smart contracts
2. Insider threats: Malicious administrators at institutions
3. Curious researchers: Attempt to re-identify data
4. Compromised participants: Submit false data
5. Government surveillance: Access data through legal processes

Attack scenarios considered:

- Key theft and impersonation
- Smart contract exploitation
- Metadata correlation and re-identification
- API attacks on access layer
- Compromise of storage infrastructure
- Sybil attacks on consensus

Limitations of our architecture:

- Relies on secure key management (not fully detailed)
- Assumes honest majority in blockchain network
- Cannot prevent data leakage by authorised users
- Does not address hardware-level attacks.

LOGISTICAL AND TECHNICAL COMPLEXITIES

The massive size of genomic datasets presents significant logistical and technical challenges. A single genome sequence can exceed 100 gigabytes, and with the growth of personalised medicine, the volume of genomic data is increasing exponentially. Stephens et al. highlight that Current storage and computational infrastructures struggle to manage these data volumes efficiently, leading to high costs and potential data loss. In addition, the lack of standardised data formats complicates collaboration between research institutions and healthcare providers. Fragmented systems make it difficult to integrate genomic data into clinical workflows or research pipelines. This issue limits the scalability of genomic data applications and delays advancements in healthcare and science [47-49],

PUBLIC AND TRUST PARTICIPATION

Trust in genomic data management is critical for fostering public participation in research and personalised medicine. However, trust has been undermined by cases of genetic surveillance and unauthorised data sharing. Clarice highlights that consumers are increasingly wary of contributing their genomic data due to fears of misuse, including tracking by governments or corporations for purposes beyond their consent. Such concerns deter people from participating in genomic studies, reducing the diversity and representativeness of datasets and limiting the potential for scientific discoveries [45-47].

REGULATORY AND ETHICAL CONSIDERATIONS

GDPR COMPLIANCE AND BLOCKCHAIN TENSIONS

The tension between blockchain immutability and GDPR rights requires explicit attention describe in Table 3.

Table 3. Blockchain immutability and GDPR rights.

Regulatory Area	Requirement / Right	Blockchain-Related Challenge	Proposed Mitigation / Consideration
GDPR – Article 17	Right to erasure	Blockchain records are immutable, making permanent deletion technically challenging	Store personal and genomic data off-chain so that they can be modified or deleted when required
GDPR – Article 16	Right to rectification	Incorrect information recorded on-chain cannot easily be modified	Store only hashes and limited metadata on-chain, while maintaining editable source data off-chain
GDPR – Article 5	Data minimisation	Storing complete genomic data on-chain may result in excessive collection or processing of personal data	Avoid storing full genomic datasets on-chain; use hashes, references, and minimum necessary metadata
Consent & Access Management	Control over personal data	Traditional consent withdrawal can be difficult in decentralised environments	Use smart contracts to support consent management and permission revocation
Privacy Protection	Protection of sensitive genomic information	Genomic data are highly sensitive and may expose information about individuals and relatives	Apply cryptographic techniques, selective disclosure, and other privacy-preserving mechanisms [45,46]
On-chain Metadata	Protection of personal data	Metadata may still be considered personal data if it can be linked to an identifiable individual	Minimise metadata and apply pseudonymisation, encryption, and privacy-preserving techniques
Data Subject Access	Right of access	Distributed storage and multiple network participants can make data retrieval and access requests difficult	Establish clear data-location, identity-management, and governance mechanisms
GDPR Chapter V	Cross-border data transfers	Decentralised networks may distribute or replicate data across different jurisdictions	Restrict data replication and implement appropriate safeguards for international transfers
Data Governance	Identification of controller/processor	Decentralised architecture can make it difficult to identify a single data controller or processor	Define roles and responsibilities through governance policies, permissioned networks, and contractual arrangements

Regulatory Area	Requirement / Right	Blockchain-Related Challenge	Proposed Mitigation / Consideration
HIPAA	Administrative, physical, and technical safeguards	Blockchain infrastructure must protect electronic protected health information (ePHI)	Implement comprehensive security controls, risk assessments, encryption, and secure infrastructure
HIPAA	Access controls and audit trails	Multiple participants may require different levels of access to genomic and clinical data	Implement role-based access controls, authentication, authorisation, and immutable audit trails
HIPAA	Business Associate Agreements (BAAs)	Blockchain service providers may handle or process protected health information	Establish BAAs with applicable blockchain/cloud/service providers before processing PHI
HIPAA	Breach notification	Distributed architectures complicate identification and management of security incidents	Establish incident-response procedures, breach detection, logging, and notification mechanisms
HIPAA Governance	Covered entities and business associates	It may be unclear which blockchain participants qualify as covered entities or business associates	Clearly define participant roles, responsibilities, and contractual obligations
HIPAA Compliance	Regulatory assurance	Limited practical experience and established guidance for HIPAA-compliant blockchain genomic systems	Conduct formal security and compliance assessments and establish documented governance controls

ETHICAL CONCERNS AND INFORMED CONSENTS

Ethical issues surrounding genomic data include informed consent, data ownership, and equitable access control. Brothers and Rothstein emphasise that many current consent processes are insufficiently transparent, leaving individuals unaware of how their data will be used, stored, or shared [26]. This lack of clarity undermines autonomy and can lead to unintended consequences, such as the commercialisation of data without fair compensation to its owners [27]. At the same time, people must develop literacy in genomic science and the associated technologies, as public understanding is critical for broad adoption and ethical use [59].

Additionally, genetic discrimination remains a persistent concern. Without robust legal protections, individuals may face exclusion from opportunities based on their genetic profiles. For example, life insurance companies could use genomic information to deny coverage or increase premiums, a practice not prohibited by existing laws like GINA [50]. Such discrimination highlights the need for stronger ethical frameworks to guide genomic data use. The management of genomic data faces critical challenges that must be addressed to unlock its potential in healthcare and research. Privacy and security risks expose individuals to identity theft, genetic discrimination, and unauthorized use. Regulatory gaps, particularly in DTC services, allow exploitation and unethical practices [49, 50].

CONCLUSION

Blockchain technology offers more than just incremental improvement; it provides the structural basis for a new ethical and operational standard in genomic data stewardship. This chapter contributes a synthesised, multidisciplinary framework that positions blockchain as an essential enabler of a future where genomic data is managed securely, transparently, and equitably. Realising this future will depend on collaborative efforts among technologists, clinicians, ethicists, and policymakers to pilot these frameworks, establish necessary standards, and build the public trust required to unlock the full, responsible potential of personalised medicine.

Authors' Contribution: PG: Conceptualization, literature search, data curation, and writing original draft. RKK: Conceptualization, methodology, literature review, and writing review and editing. AN: Literature search, data analysis, and writing original draft. RR: Literature search, data curation, and writing review and editing. RKK: Conceptualization,

supervision, critical revision of the manuscript, and writing review and editing. AO: Supervision, validation, critical review, and final approval of the manuscript. All authors read and approved the final manuscript.

Conflict of Interest: The author declares no potential conflict of interest.

Source of Funding: This work has not received any financial support.

Ethical Statement: This study does not contain any studies with human subjects or animals.

Data availability: All the data supporting the results of this study are included in the article.

REFERENCES

1. Shabani M. Blockchain-based platforms for genomic data sharing: a de-centralized approach in response to the governance problems? *J Am Med Inform Assoc.* 2018;25(11):1412-1416. doi:10.1093/jamia/ocy149.
2. Ozercan HI, Ileri AM, Ayday E, Alkan C. Realizing the potential of blockchain technologies in genomics. *Genome Res.* 2018;28(9):1255-1263. doi:10.1101/gr.207464.116.
3. Benchoufi M, Ravaud P. Blockchain technology for improving clinical research trials. *Trials.* 2017;18:335. doi:10.1186/s13063-017-2035-z.
4. Albalwy F, Brass A, Davies A. A blockchain-based dynamic consent architecture to support clinical genomic data sharing (ConsentChain): proof-of-concept study. *JMIR Med Inform.* 2021;9(2):e27816. doi:10.2196/27816.
5. Jin X, Zhang M, Zhou Z, Yu X. Application of a blockchain platform to manage and secure personal genomic data: a case study of LifeCODE.ai in China. *J Med Internet Res.* 2019;21(2):e13587. doi:10.2196/13587.
6. Tripathi G, Ahad M, Casalino G. A comprehensive review of blockchain technology: underlying principles and historical background with future challenges. *Decis Anal J.* 2023;8:100220. doi:10.1016/j.dajour.2023.100344.
7. Monrat AA, Schelén O, Andersson K. A survey of blockchain from the perspectives of applications, challenges, and opportunities. *IEEE Access.* 2019;7:117134-117151. doi:10.1109/ACCESS.2019.2936094.
8. Li X, Jiang P, Chen T, Luo X, Wen Q. A survey on the security of blockchain systems. *Future Gener Comput Syst.* 2020;107:841-853. doi:10.1016/j.future.2017.08.020.
9. Rehm H, Page A, Smith L, Adams JB, Alterovitz G, Babb L, et al. GA4GH: international policies and standards for data sharing across genomic research and healthcare. *Cell Genomics.* 2021;1(2):100029. doi:10.1016/j.xgen.2021.100029.
10. Wilkinson MD, Dumontier M, Aalbersberg IJ, Appleton G, Axton M, Baak A, et al. The FAIR Guiding Principles for scientific data management and stewardship. *Sci Data.* 2016;3:160018. doi:10.1038/sdata.2016.18.
11. Brothers KB, Rothstein MA. Ethical, legal and social implications of incorporating genomic information into electronic health records. *Genet Med.* 2015;17(7):627-632. doi:10.1038/gim.2014.200.
12. Bonomi L, Huang Y, Ohno-Machado L. Privacy challenges and research opportunities for genomic data sharing. *Nat Genet.* 2020;52(6):646-654. doi:10.1038/s41588-020-0651-0.
13. Davis-Turak J, Courtney SM, Hazard E, Glen WB Jr, da Silveira WA, Wesselman T, et al. Genomics pipelines and data integration: challenges and opportunities in the research setting. *Expert Rev Mol Diagn.* 2017;17(3):225-237. doi:10.1080/14737159.2017.1282822.
14. Gymrek M, McGuire AL, Golan D, Halperin E, Erlich Y. Identifying personal genomes by surname inference. *Science.* 2013;339(6117):321-324. doi:10.1126/science.1229566.
15. Yakubu A, Chen Y-PP. Ensuring privacy and security of genomic data and functionalities. *Brief Bioinform.* 2020;21(2):511-526. doi:10.1093/bib/bbz013.
16. Albalwy F, McDermott JH, Newman WG, Brass A, Davies A. A blockchain-based framework to support pharmacogenetic data sharing. *Pharmacogenomics J.* 2022;22:1-12. doi:10.1038/s41397-022-00285-5.

-
17. Javed IT, Lemieux VL, Regier DA. SecureConsent: a blockchain-based dynamic and secure consent management for genomic data sharing. In: 2024 International Conference on Smart Applications, Communications and Networking (SmartNets). IEEE; 2024:1-6. doi:10.1109/SmartNets61466.2024.10577693.
 18. Adanur Dedetürk B, Soran A, Bakir-Güngör B. Blockchain for genomics and healthcare: a literature review, current status, classification and open issues. *PeerJ*. 2021;9:e12130. doi:10.7717/peerj.12130.
 19. Park Y-H, Kim Y, Shim J. Blockchain-based privacy-preserving system for genomic data management using local differential privacy. *Electronics*. 2021;10(23):2991. doi:10.3390/electronics10233019.
 20. Shao S, Zhang L, Wan Z, Vorobeychik Y, Kantarcioglu M, Malin B. Secure sharing and searching of genomic data using blockchain and distributed ledger technologies. *IEEE Trans Comput Biol Bioinform*. 2020;18(6):2667-2678. doi:10.1109/TCBB.2020.2990402.
 21. Aziz MMA, Sadat MN, Alhadidi D, Wang S, Jiang X, Brown CL, et al. Privacy-preserving techniques of genomic data—a survey. *Brief Bioinform*. 2019;20(3):887-895. doi:10.1093/bib/bbx139.
 22. Vavekanand R. Data security and privacy in genomics research: a comparative analysis to protect confidentiality. *Stud Med Health Sci*. 2024;5(1):1-10. doi:10.48185/smhs.v1i1.1158.
 23. Oliva A, Kaphle A, Reguant R, Smith A, Jones B, Lee C, et al. Future-proofing genomic data and consent management: a comprehensive review of technology innovations. *GigaScience*. 2024;13(1):giae021. doi:10.1093/gigascience/giae021.
 24. Hendricks-Sturup RM, Lu CY. Direct-to-consumer genetic testing data privacy: key concerns and recommendations based on consumer perspectives. *J Pers Med*. 2019;9(2):25. doi:10.3390/jpm9020025.
 25. Moneer MM, Elhoseny M, Rho S. Privacy-preserving techniques for genomic data: a survey. *IEEE Access*. 2021;9:111336-111352. doi:10.1109/ACCESS.2021.3102345.
 26. Hasselgren A, Wan P, Horn M, Kralevska K, Gligoroski D, Faxvaag A. GDPR compliance for blockchain applications in healthcare. *arXiv preprint arXiv:2009.12741*. 2020. doi:10.48550/arXiv.2009.12913.
 27. Merlec MM, Lee YK, Hong S, In H. A smart contract-based dynamic consent management system for personal data usage under GDPR. *Sensors*. 2021;21(23):7992. doi:10.3390/s21237994.
 28. Stephens ZD, Lee SY, Faghri F, Campbell RH, Zhai C, Efron MJ, et al. Big Data: astronomical or genomics? *PLoS Biol*. 2015;13(7):e1002195. doi:10.1371/journal.pbio.1002195.
 29. Rao AK. Big data in genomics: managing and analyzing large-scale clinical and proteomic data. *Int J Res Appl Sci Eng Technol*. 2025;13(3):1-12. doi:10.22214/ijraset.2025.68053.
 30. Ceri S, Pinoli P. Data science for genomic data management: challenges, resources, experiences. *SN Comput Sci*. 2019;1(4):1-10. doi:10.1007/s42979-019-0005-0.
 31. Clarice M. Genetic surveillance and data sharing: public trust implications. *J Health Polit Policy Law*. 2024;49(2):215-238. doi:10.1215/03616878-11082345. [Note: Author name and details may need verification; kept as per your original.]
 32. Middleton A, Milne R, Almarri M, Anwer S, Atutornu J, Baranova E, et al. Global public perceptions of genomic data sharing: what shapes the willingness to donate DNA and health data? *Am J Hum Genet*. 2020;107(4):743-752. doi:10.1016/j.ajhg.2020.08.023.
 33. Milne R, Morley K, Howard H, Niemiec E, Nicol D, Critchley C, et al. Trust in genomic data sharing among members of the general public in the UK, USA, Canada and Australia. *Hum Genet*. 2019;138(11-12):1237-1246. doi:10.1007/s00439-019-02062-0.
 34. Kleeman K. Do your genes fit: how life insurance companies discriminate based on genetic test results. *J Biosecure Biosaf Biodef Law*. 2024;14(1). doi:10.1515/jbbbl-2023-0005.
 35. Shaikh M, Ebrahimi A, Wiil U. A novel blockchain-based model for secure genomic data management. *Stud Health Technol Inform*. 2025. doi:10.3233/SHTI250724.

-
36. Musamih A, Salah K, Jayaraman R, Ellaham S, Omar M, Yaqoob I. Blockchain and NFT-based solution for genomic data management, sharing, and monetization. *IEEE Access*. 2025;13:35780-35804. doi:10.1109/ACCESS.2025.3544643.
 37. Pattengale ND, Hudson CM. Blockchain-based approaches to genomic data privacy and security. *Front Genet*. 2020;11:570. doi:10.3389/fgene.2020.00570.
 38. Wan Z, Hazel J, Clayton E, Vorobeychik Y, Kantarcioglu M, Malin B. Sociotechnical safeguards for genomic data privacy. *Nat Rev Genet*. 2022;23(4):215-228. doi:10.1038/s41576-022-00455-y.
 39. Jaiman V, Urovi V. A consent model for blockchain-based health data sharing platforms. *IEEE Access*. 2020;8:140077-140093. doi:10.1109/ACCESS.2020.3014565.
 40. Nugent T, Upton D, Cimpoesu M. Improving data transparency in clinical trials using blockchain smart contracts. *F1000Research*. 2016;5:2541. doi:10.12688/f1000research.9756.1.
 41. Choudhury O, Sarker H, Rudolph N, Foreman M, Fay N, Dhuliawala M, et al. Enforcing human subject regulations using blockchain and smart contracts. *Blockchain Healthc Today*. 2018;1. doi:10.30953/bhty.v1.10.
 42. Kostick-Quenet K, Corrales Compagnucci M, Aboy M, Minssen T. Patient-centric federated learning: automating meaningful consent to health data sharing with smart contracts. *J Law Biosci*. 2025;12(1). doi:10.1093/jlb/laf003.
 43. Corte-Real A, Nunes T, da Cunha PR. Reflections about blockchain in health data sharing: navigating a disruptive technology. *Int J Environ Res Public Health*. 2024;21(2):1234. doi:10.3390/ijerph21020230.
 44. Reegu F, Al-khateeb M, Zogaan W, Al-Mousa M, Alam S, Al-Shourbaji I, et al. Blockchain-based framework for interoperable electronic health records for an improved healthcare system. *Sustainability*. 2023;15(7):6001. doi:10.3390/su15076001.
 45. Agbo CC, Mahmoud QH, Eklund JM. Blockchain technology in healthcare: a systemic review. *Healthcare*. 2019;7(2):56. doi:10.3390/healthcare7020056.
 46. Annupriya, Kumar R. A review of blockchain technology for secure and transparent healthcare systems. In: *Proceedings of the 2025 International Conference on Engineering Innovations and Technologies (ICoEIT)*. IEEE; 2025:381-386. doi:10.1109/ICoEIT63558.2025.11211691.
 47. Taddese A, Addis AC, Tam BT. Data stewardship and curation practices in AI-based genomics and automated microscopy image analysis for high-throughput screening studies: promoting robust and ethical AI applications. *Hum Genomics*. 2025;19(1):1-18. doi:10.1186/s40246-025-00716-x.
 48. Etchegary H, Darmonkov G, Simmonds C, Pullman D, Rahman P. Public attitudes towards genomic data sharing: results from a provincial online survey in Canada. *BMC Med Ethics*. 2023;24:67. doi:10.1186/s12910-023-00937-2.
 49. He K, Ge D, He MM. Big data analytics for genomic medicine. *Int J Mol Sci*. 2017;18(2):412. doi:10.3390/ijms18020412.
 50. Tanjo T, Kawai Y, Tokunaga K, Ogasawara O, Nagasaki M. Practical guide for managing large-scale human genome data in research. *J Hum Genet*. 2020;65(10):849-857. doi:10.1038/s10038-020-00862-1.