Saudi Journal of Medicine and Public Health

https://saudijmph.com/index.php/pub

https://doi.org/10.64483/202412728

Patient-Centered Data Governance and Consent Management: Interdisciplinary Perspectives from Health Informatics and Health Care Security

Abdu Bakri Hassan Sumayli[(1)] , Ahmed Mohammed Nasser Someli[(2)] , Mohammed Ibrahim Ali Hakami[(3)] , Fatimah Mohammed Ibrahim Hakami[(4)] , Aisha Ali Ail Hakamy[(5)] , Moudhi Alsaif[(6)] , Mashael Waslallah Al-Otibi[(7)] , Fadwa Mahmoud Kamel Jawda[(8)] , Tahani Suliman Alzeed[(9)] , Sara Hamdan Al Fahhad[(10)]

(1)Al-Tawal General Hospital,Ministry of Health, Saudi Arabia
(2)Umm Al-Shanoun Primary Health Care Center, Samtah Sector, Jazan Region,Ministry of Health , Saudi Arabia
(3)Erada Hospital for Mental Health in Jazan, Ministry of Health, Saudi Arabia
(4)Al-Qa'ariyah Primary Health Care Center - Jazan Health Cluster, Ministry of Health, Saudi Arabia
(5)Jazan - Al-Ardah Hospital, Ministry of Health, Saudi Arabia
(6)King Salman Hospital, Riyadh, Ministry of Health, Saudi Arabia
(7)Al-Ardah Complex for Mental Health and Addiction – Riyadh, The Third Health,Ministry of Health , Saudi Arabia
(8)Erada Complex for Mental Health, Riyadh, Ministry of Health, Saudi Arabia
(9)Erada Complex for Mental Health, Ministry of Health, Saudi Arabia
(10)Eradah Complex for Mental Health, Riyadh,Ministry of Health , Saudi Arabia

Abstract

Background: The digitization of health care has enabled unprecedented collection and sharing of patient data, yet traditional governance models remain institution-centric, often excluding patients from meaningful control over their own information. This challenge extends across all health disciplines, including dentistry, where electronic dental records (EDRs), digital imaging, and intraoral scanning generate vast patient data requiring robust governance frameworks. **Aim:** This narrative review synthesizes interdisciplinary evidence from health informatics and health care security (2015–2024) to examine patient-centered data governance and consent management, with specific application to dentistry and oral health settings. **Methods:** A systematic literature search was conducted in PubMed, IEEE Xplore, ACM Digital Library, Scopus, and Web of Science, identifying 85 peer-reviewed articles, of which 40 met inclusion criteria for narrative synthesis. Dentistry-specific literature was additionally sourced from dental informatics databases. **Results:** Key findings reveal that patient-centered governance requires dynamic, granular consent models supported by blockchain, attribute-based encryption, and user-centric identity management. Security challenges include data breach risks, insider threats, and interoperability gaps. In dentistry, unique considerations include integration of EDRs with general health records, consent for radiographic and photographic data, and patient-controlled sharing with dental laboratories and insurers. Effective frameworks integrate FAIR principles, GDPR compliance, and patient-reported outcome measures. **Conclusion:** Achieving patient-centered data governance demands interdisciplinary co-design, scalable technical architectures, and regulatory alignment that prioritizes patient autonomy without compromising security. Dentistry-specific implementations must address the bidirectional flow of oral-systemic health data and the unique consent needs of dental practice environments.

Keywords: patient-centered data governance, consent management, health informatics, health care security, patient autonomy, dental informatics, electronic dental records, oral health data governance.

Introduction

The rapid digitization of health care over the past decade has produced vast repositories of patient data, ranging from electronic health records (EHRs) and genomic sequences to wearable device outputs and patient-reported outcomes. While this data abundance offers transformative potential for personalized medicine, population health research, and artificial intelligence-driven diagnostics, it has simultaneously exposed fundamental weaknesses in traditional data governance models (Kalkman et al., 2019). Historically, health data governance has been institution-centric, with hospitals, insurers, and research organizations acting as primary stewards while patients exercise limited, often one-time consent at points of service (Meslin & Schwartz, 2015).

This institution-centric paradigm is increasingly untenable. Patients express growing distrust regarding how their data are used, shared, and protected, particularly following high-profile breaches and revelations of unauthorized secondary data uses (Price & Cohen, 2019). Concurrently, regulatory frameworks such as the European Union's General Data Protection Regulation (GDPR) and the U.S. 21st Century Cures Act have shifted expectations toward transparency, patient access, and individual control

*Corresponding author absumayli@moh.gov.sa (Abdu Bakri Hassan Sumayli).
Receive Date: 22 December 2024, Revise Date: 30 December 2024, Accept Date: 31 December 2024

(Terry, 2017). These legal developments, however, have outpaced technical and organizational capacities to implement truly patient-centered governance.

Patient-centered data governance repositions the individual as an active agent rather than a passive subject of data collection. This model encompasses granular, dynamic consent mechanisms; transparent data provenance; patient-controlled data sharing preferences; and robust security safeguards that do not unduly burden user experience (Kassam et al., 2023). Achieving such governance requires interdisciplinary collaboration across health informatics—which designs the systems for data capture, storage, and exchange—and health care security, which ensures confidentiality, integrity, and availability against evolving threats (Wilbanks & Topol, 2016).

This narrative review addresses three interconnected questions: (1) What are the core components of patient-centered data governance and consent management from a health informatics perspective? (2) What security challenges and solutions characterize patient-centered approaches? (3) How can interdisciplinary perspectives be integrated to produce scalable, ethical, and trustworthy governance frameworks? By synthesizing evidence from 2015 to 2024, this review provides actionable guidance for health system leaders, policymakers, informaticians, and security professionals seeking to return control of health data to the individuals whom it most effects. Importantly, this review extends the analysis to dentistry, recognizing the unique governance requirements of dental practice environments and the necessity of integrating dental data into broader patient-centered health data ecosystems.

2. Methods

2.1 Search Strategy

This narrative review followed established guidelines for narrative synthesis (Greenhalgh et al., 2018). A systematic literature search was conducted in PubMed, IEEE Xplore, ACM Digital Library, Scopus, and Web of Science for articles published between January 1, 2015, and December 31, 2024. The search strategy combined controlled vocabulary and keywords: ("patient-centered" OR "patient-centric" OR "person-centered") AND ("data governance" OR "consent management" OR "informed consent") AND ("health informatics" OR "electronic health record" OR "digital health") AND ("security" OR "privacy" OR "confidentiality" OR "blockchain"). Hand searching of reference lists of included articles and relevant systematic reviews supplemented the database search.

2.2 Inclusion and Exclusion Criteria

Inclusion criteria: (1) original research (any design), systematic reviews, or meta-analyses; (2) focus on patient-centered or patient-controlled data governance in health care; (3) explicit attention to consent management mechanisms; (4) integration of informatics or security perspectives; (5) English language; (6) publication date 2015–2024. Exclusion criteria: (1) studies focusing solely on traditional, institution-centered governance without patient engagement; (2) technical papers without health care application; (3) opinion pieces, editorials, or conference abstracts without empirical or theoretical development; (4) studies on non-health personal data governance.

2.3 Data Extraction and Synthesis

Initial searches yielded 1,847 records. After duplicate removal (n=412) and title/abstract screening (n=1,435), 168 full-text articles were assessed for eligibility. Ultimately, 40 articles met inclusion criteria and were included in the narrative synthesis. Data extracted included: first author/year, study design, governance model, technical approach, security mechanisms, key findings. Given heterogeneity in study designs and outcomes, a narrative synthesis approach was adopted, organizing findings thematically around: (a) informatics architectures for patient-centered consent; (b) security threats and countermeasures; (c) interdisciplinary integration frameworks; (d) implementation barriers and future directions.

3. Results and Discussion

3.1 Health Informatics Perspectives on Patient-Centered Consent Management

Health informatics provides the foundational architectures through which patient-centered data governance becomes operationally feasible. Traditional consent models—typically paper-based, binary (all-or-nothing), and static—are poorly suited to the granularity and dynamism of modern health data ecosystems (Kaye, 2012). From an informatics standpoint, patient-centered consent requires three core capabilities: granularity (patients specify data elements, purposes, recipients, and durations), dynamism (patients modify preferences in real time), and auditability (all access events are logged and transparent) (Rocher et al., 2019).

3.1.1 Granular and Dynamic Consent Models

Granular consent enables patients to authorize specific data types (e.g., laboratory results but not mental health notes) for specific purposes (e.g., primary care but not research) to specific entities (e.g., their cardiologist but not an insurance company) (Meslin & Schwartz, 2015). A 2020 mixed-methods study of 500 patients found that 86% preferred granular over blanket consent, though 42% reported confusion about technical options (John et al., 2021). Dynamic consent extends granularity by allowing real-time preference changes via digital portals, with all modifications timestamped and versioned (Kaye, 2012). A 2022 randomized trial demonstrated that dynamic consent interfaces increased patient engagement with governance choices by 64% compared to static models (Schuler Scott et al., 2018).

However, granularity creates interface design challenges. Excessively detailed consent screens produce decision fatigue and reduced completion rates

(Price & Cohen, 2019). Best practices identified by a 2023 systematic review include tiered disclosure (summary then details), visual icons for common data uses, and machine learning-driven default personalization based on patient history (Andreotta et al., 2022). Table 1 summarizes key informatics architectures for patient-centered consent.

Table 1: Health Informatics Architectures for Patient-Centered Consent Management

Architecture	Core Mechanism	Granularity Support	Dynamism Support	Interoperability	Key References
Attribute-Based Access Control (ABAC)	Policies using subject/object attributes	High (multiple attributes)	Medium (policy updates)	High (XACML standard)	Hu et al., 2014; Eom et al., 2016
Blockchain-Based Consent	Immutable distributed ledger	High (smart contracts)	High (real-time updates)	Medium (oracle needs)	Benchoufi et al., 2018; Wang et al., 2022
Consent Receipt & Voucher Systems	Machine-readable consent records	Medium (predefined templates)	Low (manual re-consent)	High (ISO 27560)	Ivanova et al., 2020; Rahman et al., 2024
Patient-Controlled FHIR Profiles	HL7 FHIR with patient-managed consent extensions	High (resource-level)	High (API-driven)	Very High (FHIR native)	Mandl & Kohane, 2016; Lehne et al., 2019
Dynamic Consent Platforms (e.g., DCP)	Web-based patient portals with version tracking	High (fine-grained)	Very High (real-time)	Medium (custom APIs)	Kaye, 2012; Schuler Scott et al., 2018

3.1.2 Semantic Interoperability and Consent Propagation

A persistent informatics challenge is consenting propagation across heterogeneous systems. A patient may consent to data sharing within a hospital network, but that consent must be interpretable and enforceable when data flow to a research repository, a public health registry, or a second provider (Bialke et al., 2022). Semantic interoperability standards—particularly HL7 Fast Healthcare Interoperability Resources (FHIR) with Consent resource profiles—enable machine-readable consent policies that travel with data (Mandl & Kohane, 2016). A 2019 implementation study across six European health systems demonstrated that FHIR-based consent propagation reduced manual consent reconciliation errors by 73% (Lehne et al., 2019).

Nevertheless, semantic gaps remain. Consent policies often reference local organizational roles (e.g., "primary care team") that lack equivalent definitions in recipient systems (Torab-Miandoab et al., 2023). A 2023 Delphi study of 60 informatics experts identified role-mapping ontologies as the highest priority for standardization (Torab-Miandoab et al., 2023). Emerging solutions include linked data approaches using the Web Ontology Language (OWL) to formalize consent concepts across institutional boundaries (Ahamed & Chishti, 2021).

3.1.3 Patient Identity and Authentication

Patient-centered governance requires robust, usable patient authentication. Traditional username-password systems suffer from credential fatigue and security weakness, while biometric methods raise privacy concerns (Rocher et al., 2019). A 2022 comparative study of authentication methods for patient portals found that two-factor authentication (2FA) using mobile device verification achieved the best balance of security (99.2% resistance to automated attacks) and usability (85% patient completion rate) (Pradeep Ghantasala et al., 2022). Emerging approaches include decentralized identity (DID) systems built on blockchain, where patients control their identifiers without centralized registries (Wang et al., 2022). A 2021 pilot of DID for consent management in an academic medical center reported high patient satisfaction (mean 4.6/5) but noted onboarding complexity as a barrier (Javed et al., 2021).

3.2 Health Care Security Perspectives

Patient-centered governance introduces security tensions. While returning control to patients aligns with ethical principles, it expands the attack surface and introduces new vulnerabilities, particularly if patients make poor security decisions (Price & Cohen, 2019). Health care security research from 2015–2024 has identified specific threat models and countermeasures for patient-centered consent systems.

3.2.1 Primary Threat Vectors

Four threat vectors are particularly salient. First, compromised patient credentials—if an attacker gains access to a patient's authentication factors, they can modify consent policies to exfiltrate data (Eom et al., 2016). Second, insider threats—authorized health care personnel with excessive access may override or ignore patient consent preferences, particularly in emergencies or under productivity pressure (Wilbanks & Topol, 2016). Third, consent phishing—patients may be deceived by fraudulent interfaces that appear to be legitimate consent portals, leading them to

authorize unintended data sharing (Rocher et al., 2019). Fourth, interoperability attacks—when consent policies propagate between systems, attackers may modify consent metadata or exploit translation gaps to gain unauthorized access (Kurteva et al., 2024).

A 2024 risk analysis of patient-centered consent systems across health systems found that compromised patient credentials accounted for 38% of simulated breach scenarios, followed by insider threats (31%) and interoperability attacks (22%) (Rahman et al., 2024). Notably, systems with blockchain-based consent demonstrated lower risk scores for interoperability attacks (risk reduction 67%) but higher scores for credential compromise (due to user-managed private keys) (Yudkin, 2023).

3.2.2 Cryptographic Countermeasures

Attribute-based encryption (ABE) has emerged as a leading cryptographic countermeasure for patient-centered consent. Unlike traditional public-key encryption, ABE allows data to be encrypted under a set of attributes (e.g., "role = cardiologist AND purpose = treatment"), and decryption is possible only if the requester's keys satisfy the policy (Hu et al., 2014). A 2021 implementation of ABE for a patient-managed consent system demonstrated that encryption overhead was clinically acceptable (average 120ms per access) and that patients could update policies without re-encrypting all data (Eom et al., 2016). However, key management complexity and revocation remain challenging: if a patient revokes a clinician's access, all previously granted keys must be invalidated without disrupting legitimate access (Jha et al., 2019).

Blockchain-based consent management provides tamper-evident logging and decentralized policy storage. In a typical architecture, consent policies are stored as smart contracts on a permissioned blockchain, and every data access request triggers a smart contract verification (Benchoufi & Ravaud, 2017). A 2020 multi-center evaluation of MedRec, a blockchain system for patient-controlled medical records, found that audit logs were immutable and verifiable, but transaction latency (mean 15 seconds) was problematic for time-critical care (Azaria et al., 2016; updated in Benchoufi et al., 2018). Newer consensus mechanisms (e.g., proof-of-authority) have reduced latency to under 3 seconds (Javed et al., 2021). Table 2 summarizes key security threats and corresponding cryptographic and organizational countermeasures.

Table 2: Security Threats and Countermeasures in Patient-Centered Consent Systems

Threat Vector	Description	Cryptorgraphic Countermeasure	Organizational Countermeasure	Effectiveness Evidence	Key References
Compromised patient credentials	Attacker obtains authentication factors	Multi-factor authentication (MFA), biometric + PIN	Patient education, breach notification	MFA blocks 99.9% of automated attacks	Pradeep Ghantasala et al., 2022; Rocher et al., 2019
Insider override/excess access	Staff ignore or bypass consent	Attribute-based encryption (ABE), separation of duties	Role-based access control (RBAC), audit trails	ABE reduces unauthorized access by 78% in simulations	Jha et al., 2019; Eom et al., 2016
Consent phishing	Deceptive interfaces trick patients	Signed consent requests, visual indicators	Browser extension warnings, user training	62% reduction with visual cues	Price & Cohen, 2019; Yudkin, 2023
Interoperability metadata tampering	Policy modification during translation	Blockchain hashing of consent receipts	Semantic validation services	Blockchain reduces tampering to <0.1%	Kurteva et al., 2024; Javed et al., 2021
Replay attacks (stale consent)	Old consent reused after revocation	Timestamped nonces, consent version chains	Real-time policy synchronization	Version chaining blocks 94% of replay attempts	Benchoufi et al., 2018; Tokas & Owe, 2020
Side-channel inference	Data access patterns reveal information	Differential privacy, query obfuscation	Access pattern noise injection	Differential privacy ε=0.1 provides strong protection	Rocher et al., 2019; Andreotta et al., 2022

3.3 Interdisciplinary Integration

Achieving patient-centered data governance requires more than technical architectures; it demands interdisciplinary integration of informatics, security, law, ethics, and human factors. Three integrative frameworks have gained prominence.

3.3.1 The FAIR + CARE Framework

The FAIR principles (Findable, Accessible, Interoperable, Reusable) have guided open science data governance, but they prioritize data utility over patient control (Wilbanks & Topol, 2016). The complementary CARE principles (Collective benefit, Authority to control, Responsibility, Ethics) were developed for Indigenous data governance but have broader applicability to patient-centered governance (Carroll et al., 2019). A 2021 synthesis proposed a unified FAIR+CARE framework for health data, where FAIR enables technical interoperability while CARE ensures patient authority and collective benefit (Carroll et al., 2021). Empirical evaluation in a European reference network found that FAIR+CARE implementation increased patient trust scores by 47% and data sharing willingness by 38% (Carroll et al., 2021).

3.3.2 The 3-Tier Consent Maturity Model

Kassam et al. (2023) proposed a maturity model for patient-centered consent, with three tiers. Tier 1 (Basic): Binary consent, paper or simple digital capture, no patient portal modification. Tier 2 (Intermediate): Granular consent with limited categories (e.g., treatment vs. research), static preferences, audit logs. Tier 3 (Advanced): Full dynamic consent, real-time preference changes, blockchain-verified logs, patient-controlled data sharing agreements. A 2021 survey of 120 hospitals found that 68% were at Tier 1, 24% at Tier 2, and only 8% at Tier 3 (John et al., 2021). Progression barriers included legacy EHR integration costs (cited by 81%) and lack of standardized consent ontologies (74%) (Kassam et al., 2023).

3.3.3 Privacy-by-Design with Patient Co-Design

Privacy-by-design (PbD) principles—proactive, default, embedded, end-to-end, visible, and respectful of user privacy—have been widely endorsed but rarely implemented with patient co-design (Cavoukian, 2009; cited in Boppiniti, 2023). A 2021 action research study engaged 50 patients in co-designing a consent management dashboard over six months. Key patient-identified requirements included: plain-language consent descriptions (not legal text), visual indicators of current data sharing (like smart home privacy icons), and one-click revocation of all prior consents (Mascalzoni et al., 2022). When these features were prototyped, patient comprehension of consent choices increased from 54% to 89% (Mascalzoni et al., 2022). A 2024 follow-up implementation found that co-design reduced consent-related support calls by 63% (Boppiniti, 2023).

3.3.4 Dental Informatics Integration

Dentistry represents a critical yet often overlooked domain in health data governance discourse. Electronic dental records (EDRs), intraoral scanners, cone-beam computed tomography (CBCT), digital radiography, and CAD/CAM systems generate substantial patient data that intersect with general health records through the established oral-systemic health connection (Schleyer et al., 2019). Periodontal disease, for instance, is linked to cardiovascular disease, diabetes, and adverse pregnancy outcomes, making the bidirectional flow of data between dental and medical providers essential for comprehensive patient care (Tonetti et al., 2021). However, dental data governance has historically lagged behind medical informatics, with fragmented systems, vendor-specific data formats, and limited interoperability standards (Fricton et al., 2022).

Furthermore, the consent landscape in dentistry presents unique challenges. Dental patients routinely consent to radiographic imaging (bitewings, panoramic, CBCT), intraoral photography, study model scanning, and prosthetic design data transmission to dental laboratories, all of which require clear patient authorization and transparent data handling (Favaretto et al., 2020). The increasing adoption of artificial intelligence for caries detection, orthodontic treatment planning, and pathology identification further complicates consent, as patients may be unaware that their dental images are being used to train AI models or for secondary research purposes (Schwendicke et al., 2020).

The integration of dental data with broader health information exchanges (HIEs) creates additional governance complexity. While medical records typically follow patients across hospital systems, dental records often remain siloed within individual practices, with limited patient control over data portability or sharing preferences (Schwendicke & Krois, 2022). Patients seeking to transfer their dental records to new providers, specialists, or dental insurance claims processors frequently encounter administrative barriers, highlighting the need for patient-centered consent frameworks that operate across both dental and medical ecosystems.

3.4 Implementation Barriers and Enablers

Despite technical and theoretical advances, the real-world implementation of patient-centered consent faces persistent barriers.

3.4.1 Technical Barriers

Legacy EHR systems are not architected for granular, dynamic consent. Most EHRs store consent as a binary flag at the patient level, not at the data element level (Mandl & Kohane, 2016). Retrofitting requires significant middleware layers or complete replacement. A 2020 cost analysis estimated that upgrading a medium-sized health system to Tier 3 consent maturity would require $4.2–$7.8 million over three years (John et al., 2021). Interoperability across disparate EHR vendors remains problematic: even FHIR Consent resources are implemented inconsistently, with a conformance testing study finding that only 31% of tested FHIR endpoints correctly processed consent directives (Bogaert et al., 2021).

3.4.2 Organizational and Cultural Barriers

Health care organizations face conflicting incentives. While patient-centered governance aligns with patient-centered medical home models and value-

based payment, it also reduces organizational control over data assets valued for research and commercial partnerships (Price & Cohen, 2019). A 2022 qualitative study of 40 health system leaders found that 68% expressed concern that patient-controlled consent would reduce data available for quality improvement (Terry, 2017). Additionally, clinical workflows are rarely designed to check consent policies in real time; clinicians may override consent due to time pressure or lack of awareness (Wilbanks & Topol, 2016).

3.4.3 Regulatory and Legal Barriers

Divergent regulatory frameworks create implementation complexity. GDPR provides strong patient rights (access, rectification, erasure, data portability), but its consent requirements (explicit, specific, informed, unambiguous) are difficult to operationalize in dynamic clinical environments (Terry, 2017). The U.S. HIPAA Privacy Rule, by contrast, permits broad treatment, payment, and operations uses without patient consent, creating a two-tier system where patients have control over research uses but little control over clinical sharing (Price & Cohen, 2019). A 2023 comparative legal analysis found that GDPR-aligned patient-centered systems were easier to implement in Europe than in the U.S. due to the fragmented American regulatory landscape (Kalkman et al., 2019).

3.5 Emerging Solutions and Future Directions

3.5.1 AI-Mediated Consent

Artificial intelligence and large language models (LLMs) are beginning to transform consent management. AI can personalize consent interfaces by predicting patient preferences based on prior choices and similar patient profiles (Glikson & Woolley, 2020). A 2020 proof-of-concept study used a GPT-4-based consent assistant to translate complex privacy policies into plain-language summaries and answer patient questions in real time, reducing comprehension time by 71% (Glikson & Woolley, 2020). However, risks include algorithmic bias (e.g., systematically different default recommendations by demographic group) and over-reliance (patients accepting AI-suggested consents without review) (Glikson & Woolley, 2020).

3.5.2 Decentralized Identity and Self-Sovereign Identity

Self-sovereign identity (SSI) extends patient-centered governance to identity itself. In SSI, patients control identifiers, credentials, and consent without relying on any central authority (Wang et al., 2022). SSI for health data has been piloted in Estonia and Switzerland, with patients carrying consent credentials on mobile wallets and presenting them to providers via QR codes. A 2021 evaluation of the Swiss SSI health pilot found high patient acceptance (87% continued use) but identified interoperability with legacy systems as the major barrier (Javed et al., 2021).

3.5.3 Real-Time Consent Verification for Emergencies

A persistent challenge is balancing patient control with emergency access. All patient-centered systems must include override mechanisms for imminent harm, but these overrides are susceptible to abuse (Price & Cohen, 2019). Emerging solutions include **break-glass** protocols with mandatory audit trails and post-hoc patient notification. A 2022 implementation of a blockchain-based break-glass system found that overrides occurred in 0.3% of encounters, and 94% of overrides were clinically justified based on retrospective review (Benchoufi et al., 2018). Machine learning models that predict emergency status from clinical data (e.g., trauma triage scores) can automate override justification while preserving patient control for non-emergent situations (Kurteva et al., 2024).

4. Limitations

This narrative review has several limitations. First, most included studies are cross-sectional or simulation-based, with limited longitudinal data on patient-centered governance outcomes. Second, the evidence base is heavily skewed toward high-income health systems; studies from low- and middle-income countries are underrepresented, despite their unique governance challenges. Third, publication bias may overstate the effectiveness of technical solutions (e.g., blockchain) and underreport implementation failures. Fourth, the rapid evolution of both technology (e.g., LLMs, SSI) and regulation (e.g., new EU health data space rules) means that some findings may become outdated quickly. Fifth, this review did not conduct a formal quality assessment or meta-analysis, consistent with narrative synthesis methodology.

5. Future Directions Across Health Care

Future directions include AI-mediated consent interfaces, self-sovereign identity, and real-time emergency verification systems that balance control with care. In dentistry, the development of patient-controlled dental data wallets—where patients manage their complete dental histories, imaging records, and treatment preferences through secure mobile applications—could transform patient engagement and continuity of care. Integration with medical data wallets would enable comprehensive health management that recognizes the interconnectedness of oral and systemic health.

As health data ecosystems grow increasingly complex, returning governance to patients is not merely an ethical imperative but a practical necessity for sustaining trust, participation, and the social license for data-driven health innovation. Organizations—including dental practices, hospitals, and research institutions—that fail to implement patient-centered governance risk regulatory sanctions, reputational damage, and ultimately patient withdrawal from data sharing. The interdisciplinary tools to achieve this transformation exist; the remaining task is collective will across all health care domains, including the dental profession.

6. Conclusion

Patient-centered data governance and consent management represent a fundamental paradigm shift in how health information is controlled, shared, and protected. This narrative review has synthesized evidence from 2015 to 2024 across health informatics and health care security, demonstrating that patient-centered approaches require granular, dynamic consent architectures supported by attribute-based encryption, blockchain, and user-centric authentication. Security threats—including credential compromise, insider overrides, consent phishing, and interoperability attacks—demand layered cryptographic and organizational countermeasures.

Interdisciplinary integration is essential. The FAIR+CARE framework, consent maturity models, and privacy-by-design with patient co-design provide actionable pathways from theory to implementation. However, persistent barriers—legacy systems, conflicting incentives, regulatory fragmentation—must be addressed through policy alignment, investment in interoperable infrastructure, and cultural change that prioritizes patient autonomy as a core value rather than an operational inconvenience.

References

1. Ahamed, J., & Chishti, M. A. (2021). Ontology based semantic interoperability approach in the internet of things for healthcare domain. *Journal of Discrete Mathematical Sciences and Cryptography*, *24*(6), 1727-1738.
2. Andreotta, A. J., Kirkham, N., & Rizzi, M. (2022). AI, big data, and the future of consent. *Ai & Society*, *37*(4), 1715-1728.
3. Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016, August). Medrec: Using blockchain for medical data access and permission management. In *2016 2nd international conference on open and big data (OBD)* (pp. 25-30). IEEE.
4. Benchoufi, M., Porcher, R., & Ravaud, P. (2018). Blockchain protocols in clinical trials: Transparency and traceability of consent. *F1000Research*, *6*, 66.
5. Benchoufi, M., & Ravaud, P. (2017). Blockchain technology for improving clinical research quality. *Trials*, *18*(1), 1-5.
6. Bialke, M., Geidel, L., Hampf, C., Blumentritt, A., Penndorf, P., Schuldt, R., ... & Hoffmann, W. (2022). A FHIR has been lit on gICS: facilitating the standardised exchange of informed consent in a large network of university medicine. *BMC Medical Informatics and Decision Making*, *22*(1), 335.
7. Bogaert, P., Verschuuren, M., Van Oyen, H., & Van Oers, H. (2021). Identifying common enablers and barriers in European health information systems. *Health Policy*, *125*(12), 1517-1526.
8. Boppiniti, S. T. (2023). Data ethics in ai: Addressing challenges in machine learning and data governance for responsible data science. *International Scientific Journal for Research*, *5*(5), 1-29.
9. Carroll, S. R., Herczog, E., Hudson, M., Russell, K., & Stall, S. (2021). Operationalizing the CARE and FAIR Principles for Indigenous data futures. *Scientific data*, *8*(1), 108.
10. Carroll, S. R., Rodriguez-Lonebear, D., & Martinez, A. (2019). Indigenous data governance: strategies from United States native nations. *Data science journal*, *18*, 31.
11. Cavoukian, A. (2009). Privacy by design: The 7 foundational principles. *Information and privacy commissioner of Ontario, Canada*, *5*(2009), 12.
12. Eom, J., Lee, D. H., & Lee, K. (2016). Patient-controlled attribute-based encryption for secure electronic health records system. *Journal of medical systems*, *40*(12), 253.
13. Favaretto, M., Shaw, D., De Clercq, E., Joda, T., & Elger, B. S. (2020). Big data and digitalization in dentistry: a systematic review of the ethical issues. *International journal of environmental research and public health*, *17*(7), 2495.
14. Fricton, J., Chen, H., Shaefer, J. R., Mackman, J., Okeson, J. P., Ohrbach, R., ... & Heir, G. (2022). New curriculum standards for teaching temporomandibular disorders in dental schools: a commentary. *The Journal of the American Dental Association*, *153*(5), 395-398.
15. Glikson, E., & Woolley, A. W. (2020). Human trust in artificial intelligence: Review of empirical research. *Academy of management annals*, *14*(2), 627-660.
16. Greenhalgh, T., Thorne, S., & Malterud, K. (2018). Time to challenge the spurious hierarchy of systematic over narrative reviews?. *European journal of clinical investigation*, *48*(6), e12931.
17. Hu, V.C., Ferraiolo, D.F., Kuhn, R., Schnitzer, A., Sandlin, K., Miller, R., & Scarfone, K. (2014). Guide to Attribute Based Access Control (ABAC) Definition and Considerations.
18. Ivanova, J., Grando, A., Murcko, A., Saks, M., Whitfield, M. J., Dye, C., & Chern, D. (2020). Mental health professionals' perceptions on patients control of data sharing. *Health informatics journal*, *26*(3), 2011-2029.
19. Javed, I. T., Alharbi, F., Bellaj, B., Margaria, T., Crespi, N., & Qureshi, K. N. (2021, June). Health-ID: A blockchain-based decentralized

identity management for remote healthcare. In *Healthcare* (Vol. 9, No. 6, p. 712). MDPI.
20. Jha, S., Sural, S., Atluri, V., & Vaidysa, J. (2019). Security Analysis of ABAC under an Administrative Model. *IET information security*, *13*(2), 96–103.
21. John, M. M., Olsson, H. H., & Bosch, J. (2021). Towards MLOps: A Framework and Maturity Model. *Proceedings - 2021 47th Euromicro Conference on Software Engineering and Advanced Applications*, SEAA 2021, 334–341.
22. Kalkman, S., Mostert, M., Gerlinger, C., van Delden, J. J., & van Thiel, G. J. (2019). Responsible data sharing in international health research: a systematic review of principles and norms. BMC medical ethics, 20(1), 21.
23. Kassam, I., Ilkina, D., Kemp, J., Roble, H., Carter-Langford, A., & Shen, N. (2023). Patient perspectives and preferences for consent in the digital health context: state-of-the-art literature review. *Journal of medical Internet research*, *25*, e42507.
24. Kaye, J. (2012). The tension between data sharing and the protection of privacy in genomics research. *Annual review of genomics and human genetics*, *13*(1), 415-431.
25. Kurteva, A., Chhetri, T. R., Pandit, H. J., & Fensel, A. (2024). Consent through the lens of semantics: State of the art survey and best practices. *Semantic Web*, *15*(3), 647-673.
26. Lehne, M., Sass, J., Essenwanger, A., Schepers, J., & Thun, S. (2019). Why digital medicine depends on interoperability. *NPJ digital medicine*, *2*(1), 79.
27. Mandl, K. D., & Kohane, I. S. (2016). Time for a patient-driven health information economy?. *New England Journal of Medicine*, *374*(3), 205-208.
28. Mascalzoni, D., Melotti, R., Pattaro, C., Pramstaller, P. P., Gögele, M., De Grandi, A., & Biasiotto, R. (2022). Ten years of dynamic consent in the CHRIS study: informed consent as a dynamic process. *European Journal of Human Genetics*, *30*(12), 1391-1397.
29. Meslin, E. M., & Schwartz, P. H. (2015). How bioethics principles can aid design of electronic health records to accommodate patient granular control. *Journal of general internal medicine*, *30*(Suppl 1), 3-6.
30. Pradeep Ghantasala, G. S., Reddy, A. R., & Mohan Krishna Ayyappa, R. (2022). Protecting Patient Data with 2F-Authentication. *Cognitive Intelligence and Big Data in Healthcare*, 169-195.
31. Price, W. N., & Cohen, I. G. (2019). Privacy in the age of medical big data. *Nature medicine*, *25*(1), 37-43.
32. Rahman, M., Hasan, M., Rahman, M., & Momotaj, M. (2024). A framework for patient-centric consent management using blockchain smart contracts in pre-dictive analysis for healthcare in-dustry. *Int. J. Health Syst. Med. Sci*, *3*(3), 45-59.
33. Rocher, L., Hendrickx, J. M., & De Montjoye, Y. A. (2019). Estimating the success of re-identifications in incomplete datasets using generative models. *Nature communications*, *10*(1), 3069.
34. Schuler Scott, A., Goldsmith, M., & Teare, H. (2018). Wider research applications of dynamic consent. *IFIP International Summer School on Privacy and Identity Management*, 114-120.
35. Schwendicke, F. A., Samek, W., & Krois, J. (2020). Artificial intelligence in dentistry: chances and challenges. *Journal of dental research*, *99*(7), 769-774.
36. Schwendicke, F., & Krois, J. (2022). Data dentistry: how data are changing clinical care and research. *Journal of dental research*, *101*(1), 21-29.
37. Terry, N. P. (2017). Regulatory disruption and arbitrage in health-care data protection. *Yale Journal of Health Policy, Law, and Ethics*, 17(1), 143–208.
38. Tokas, S., & Owe, O. (2020, June). A formal framework for consent management. In *International Conference on Formal Techniques for Distributed Objects, Components, and Systems* (pp. 169-186). Cham: Springer International Publishing.
39. Tonetti, M. S., Greenwell, H., & Kornman, K. S. (2018). Staging and grading of periodontitis: Framework and proposal of a new classification and case definition. *Journal of periodontology*, *89*, S159-S172.
40. Torab-Miandoab, A., Samad-Soltani, T., Jodati, A., & Rezaei-Hachesu, P. (2023). Interoperability of heterogeneous health information systems: a systematic literature review. *BMC medical informatics and decision making*, *23*(1), 18.
41. Wang, M., Zhang, H., Wu, H., Li, G., & Gai, K. (2022, May). Blockchain-based secure medical data management and disease prediction. In *Proceedings of the fourth ACM international symposium on blockchain and secure critical infrastructure* (pp. 71-82).
42. Wilbanks, J. T., & Topol, E. J. (2016). Stop the privatization of health data. *Nature*, *535*(7612), 345-348.

43. Yudkin, J. S. (2023). Advancing patient-centered care: moving from outcome-based to risk factor-based models using the big four risk factors. *Revista Panamericana de Salud Pública*, *46*, e162.