Saudi Journal of Medicine and Public Health

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

https://doi.org/10.64483/202412517

The Paradox of Integration: A Narrative Review on the Ethics and Security of the Centralized Patient Profile in Multidisciplinary Healthcare

Fadiyah Ali Ayishi [(1)] , Ali Mohammed Al Rayiq [(2)] , Zohour Hussain Hussain Mobarki [(3)] , Yousef Abdullrahman Bajunayd [(4)] , Mohammed Nasser Qasimi [(5)] , Gasem Jaber Mohammed Alhamzi [(3)] , Najoud Zain Othman Al Hadi , Safa Mohammed Khard , Mariam Mohammed Yahya Somaily [(6)] , Asaad Munwer Al mutairi [(7)] , Almontaserbella Abdulhadi Suror [(8)] , Abdullah Abdulaziz Ibrahim Alghamdi [(8)]

(1) Alhabjia Primary Health Care. Jazan Health cluster, Ministry of Health, Saudi Arabia,
(2) Adham General Hospital, Ministry of Health, Saudi Arabia,
(3) Mawid service management, Jazan Health Cluster, Ministry of Health, Saudi Arabia,
(4) Hospital Affairs Department of Health cluster, Ministry of Health, Saudi Arabia,
(5) Mawid Services Management In Jazan Health cluster, Ministry of Health, Saudi Arabia,
(6) Maternity and Children's Hospital – Bisha, Ministry of Health, Saudi Arabia,
(7) Al Murooj Health Center, Ministry of Health, Saudi Arabia,
(8) King Abdullah Medical Complex, Ministry of Health, Saudi Arabia

Abstract

Background: The drive towards value-based, coordinated care has made the integrated Centralized Patient Profile (CPP) a cornerstone of modern health informatics. This profile aggregates deeply sensitive data from nursing narratives, epidemiological histories, genetic lab results, and administrative sources, creating a comprehensive yet ethically complex digital persona. **Aim:** This review aims to critically analyze the ethical, legal, and practical challenges inherent in managing the CPP across multidisciplinary boundaries. It focuses on the tensions between data utility for care and the imperative of privacy and security. **Methods:** A narrative synthesis methodology was employed, analyzing literature from 2010-2024 sourced from PubMed, IEEE Xplore, ACM Digital Library, and grey literature (legal, policy, and technical reports). Thematic analysis was conducted across the domains of ethics, law, security, and clinical practice. **Results:** The CPP creates a "paradox of integration": while it enhances care coordination, it simultaneously exacerbates risks of privacy harm, discriminatory misuse, and unauthorized access. Key challenges include defining the "right to know" across disciplines, protecting particularly sensitive data (genetic, social), and implementing technically robust yet clinically usable segmentation controls. Current legal frameworks like HIPAA are insufficient for governing complex, inferred data within CPPs. **Conclusion:** Realizing the CPP's promise requires a paradigm shift from monolithic data sharing to ethical, "privacy-by-design" architectures with granular, context-aware access controls. This must be underpinned by reformed policies, interdisciplinary ethics training, and a culture that balances seamless care with vigilant data stewardship.

Keywords: Integrated Patient Record, Health Information Privacy, Role-Based Access Control, Health Data Ethics, Interprofessional Communication

Introduction

The vision of a seamless, holistic patient record has driven health informatics for decades. This vision has materialized in the form of the Centralized Patient Profile (CPP), a dynamic, integrated digital repository that aggregates data from every touchpoint in the healthcare system (Keshta & Odeh, 2021). Far more than a simple medication list, the modern CPP synthesizes the narrative richness of nursing notes detailing patient vulnerabilities and psychosocial contexts; epidemiological data on travel history, occupation, and behavioral risk factors; definitive genetic and biomarker laboratory results predicting future disease; and the administrative data handled by medical secretaries, including insurance details, billing codes, and appointment histories (Caine & Tierney, 2015). This integration promises transformative benefits: reducing medical errors, eliminating redundant testing, enabling personalized medicine, and empowering patients with a unified view of their health (Adler-Milstein & Pfeifer, 2017).

However, this powerful integration creates a profound and under-examined paradox. The very comprehensiveness that makes the CPP clinically invaluable also renders it a uniquely sensitive and risky artifact. It constructs what some scholars term a "digital phenotype"—a potentially revealing and

*Corresponding author e-mail: Faishi@moh.gov.sa (Fadiyah Ali Ayishi).
Receive Date: 20 December 2024, Revise Date: 30 December 2024, Accept Date: 31 December 2024

lasting portrait that can include predictive genetic predispositions, stigmatizing lifestyle details, mental health notes, and financial information (Shaban-Nejad et al., 2018). Consequently, the CPP sits at a volatile intersection of clinical utility and ethical peril. Managing access to this profile across multidisciplinary teams—nurses, physicians, epidemiologists, lab technicians, and administrative staff—presents unprecedented challenges. Each discipline possesses a different, context-dependent "right to know," yet legacy Electronic Health Record (EHR) systems often default to broad access models that fail to segment this sensitive data appropriately (Blease et al., 2022).

This narrative review, therefore, aims to critically dissect the ethical, legal, and practical-security challenges of the CPP in multidisciplinary settings. It is guided by three core questions: (1) What are the primary ethical dilemmas and privacy harms arising from aggregating highly sensitive, multi-source data into a single profile? (2) How do current legal and regulatory frameworks govern access and use, and where do they fall short? (3) What informatics solutions, particularly in access control and data segmentation, are emerging to navigate the tension between necessary sharing and essential privacy? By synthesizing literature from bioethics, health law, cybersecurity, and clinical informatics, this review argues that realizing the promise of the CPP requires moving beyond simplistic data aggregation toward ethically architected, intelligently segmented systems governed by a renewed social contract for health data stewardship.

Methodology

To address these interdisciplinary questions, a narrative review methodology was selected to allow for the synthesis of diverse evidence streams and theoretical perspectives. A systematic search was conducted in 2024 across several databases: PubMed/MEDLINE (for clinical, ethical, and public health literature), IEEE Xplore (for technical and security-focused research), and ACM Digital Library (for privacy-enhancing technologies and human-computer interaction studies). Search strings combined terms such as ["centralized patient record" OR "integrated health record" OR "longitudinal health record"] AND ["ethics" OR "privacy" OR "security" OR "access control"] AND ["multidisciplinary" OR "interprofessional"]. The search was limited to English-language publications from 2010 to 2024 to capture the era of widespread EHR adoption and evolving data privacy concerns.

Given the applied nature of the topic, significant grey literature was incorporated, including white papers from organizations like the American Medical Informatics Association (AMIA) and the Office of the National Coordinator for Health IT (ONC), legal analyses of healthcare regulations, and reports from data protection authorities. Citation chaining was used to identify seminal works. The initial screening yielded over 200 sources, which were filtered for relevance to the core themes of ethics, law, and security in data sharing across disciplines. The final corpus was analyzed thematically. Key themes identified included: (1) Ethical Principles and Harms, (2) Legal and Regulatory Landscape, (3) Disciplinary "Right to Know," and (4) Technical Security and Segmentation Solutions. These themes structure the findings and discussion below.

Ethical Dilemmas in the Aggregated Profile

The ethical analysis of the CPP must move beyond standard discussions of confidentiality to confront the novel risks created by data aggregation and inference. Core biomedical principles—autonomy, beneficence, non-maleficence, and justice—are all strained in this context (Childress & Beauchamp, 2022).

Autonomy, Consent, and the Illusion of Control

Informed consent for data use in a CPP is often functionally impossible in its traditional sense. While patients may consent to treatment, the secondary uses of their aggregated data for population health, research, or operational analytics are typically covered by broad, blanket authorizations in HIPAA notices of privacy practices, which few patients read or understand (Ploug & Holm, 2015). The CPP enables predictive analytics and data mining that can infer sensitive information (e.g., predicting depression from medication combinations or lifestyle data) never directly disclosed by the patient, challenging the very foundation of informed consent (Cohen, 2019). This creates a significant autonomy gap, where patients lose meaningful control over the narrative and uses of their digital self (Mittelstadt & Floridi, 2016).

Non-Maleficence and the Novel Harms of Aggregated Data

The foundational biomedical principle of non-maleficence, or "do no harm," is fundamentally challenged by the unique vulnerabilities introduced by the integrated Centralized Patient Profile. The process of aggregation itself creates novel categories of privacy harm that extend far beyond traditional breaches of confidentiality. The first and most pervasive is the harm of aggregation, where individually innocuous data points—a specific prescription fill, a routine lab test order, or a residential ZIP code—become powerfully revealing when correlated and analyzed within the comprehensive CPP (Rothstein, 2016). For example, a patient's HIV status, which they may have deliberately compartmentalized, can be inferred by combining data on antiretroviral prescriptions, specific lab test orders (e.g., CD4 count), and visits to an infectious disease specialist, even if the diagnosis is never explicitly documented in a progress note. This inferential exposure strips patients of their ability to control sensitive personal narratives,

turning the record meant for their care into a tool of unintended disclosure.

Beyond exposure, the CPP significantly amplifies the risk of discriminatory harm. Particularly sensitive data segments, such as predictive genetic markers indicating predisposition to costly conditions, detailed nursing narratives on lifestyle choices, or occupational histories tied to environmental exposures, become vectors for misuse (Lenartz et al., 2021). While the Genetic Information Nondiscrimination Act (GINA) offers some protection against health insurer and employer discrimination based on genetic data, these safeguards do not extend to life, disability, or long-term care insurance, leaving critical gaps (Prince & Roche, 2021). Perhaps more insidiously, this same rich data can fuel biased clinical decision-making within healthcare itself, as evidenced by studies showing how algorithmic tools or provider perceptions based on historical data can lead to inequitable treatment recommendations for certain demographic groups (Obermeyer et al., 2019). The CPP thus centralizes the very information that can facilitate both institutional and interpersonal discrimination.

Finally, the integrated record can directly engender stigmatization and self-stigma, causing psychosocial and clinical harm. The open documentation of sensitive issues such as substance use disorders, sexual health history, or mental health diagnoses in a widely accessible record can negatively alter provider attitudes and behavior. Research in nursing and medical literature documents that such transparency can lead to "diagnostic overshadowing," where a patient's somatic complaints are dismissed as behavioral, or to the unconscious provision of a lower standard of care based on stigmatizing labels (Hornum et al., 2023). This phenomenon can also trigger internalized shame or self-stigma in patients, who may avoid seeking necessary care if they believe past disclosures will lead to judgmental treatment in future clinical encounters. Therefore, the CPP, in its quest for comprehensive insight, can paradoxically undermine therapeutic relationships and exacerbate health disparities for already vulnerable populations.

Justice and the Digital Divide

The benefits of CPPs and the protections against their risks are not equitably distributed. Vulnerable populations—those with complex chronic conditions, mental health issues, or lower health literacy—generate more data, creating denser, more revealing profiles and thus bearing disproportionate privacy risk (Veinot et al., 2018). Furthermore, these groups may have less capacity to navigate complex privacy settings or advocate for their preferences, exacerbating existing health inequities.

The Legal and Regulatory Quagmire: HIPAA's Inadequacy

The primary legal framework in the United States, the Health Insurance Portability and Accountability Act (HIPAA) of 1996, is ill-equipped for the realities of the modern CPP (Cohen & Mello, 2018).

The "Treatment, Payment, and Operations" (TPO) Loophole

HIPAA permits disclosure of Protected Health Information (PHI) without specific patient authorization for purposes of treatment, payment, and healthcare operations—a category defined so broadly that it can encompass much of the data sharing within a large health system (Shahid et al., 2022). This means a billing coder in the administrative wing may, under HIPAA, have legitimate access to a patient's full clinical narrative and genetic test results if those data are embedded in the record used for billing compliance, blatantly violating the principle of least privilege (Brkić et al., 2023).

The Challenge of "De-Identification" and Re-identification

HIPAA's "safe harbor" method for de-identification, which involves removing 18 specific identifiers, is increasingly obsolete (Table 1). The rich, longitudinal data in a CPP makes re-identification through linkage with other public or commercial data sets a significant risk (Rocher et al., 2019). Furthermore, data deemed "de-identified" under HIPAA can still be used for secondary purposes (e.g., research, commercial development) without patient consent, raising ethical questions about data stewardship and the commodification of patient-derived information (Staunton et al., 2019).

Sector-Specific Laws and a Patchwork of Protections

Other laws provide sporadic, incomplete coverage. The Genetic Information Nondiscrimination Act (GINA, 2008) prohibits health insurer and employer discrimination but does not cover life, disability, or long-term care insurance (Prince & Roche, 2021). State laws vary widely, and federal regulations for substance use disorder records (42 CFR Part 2) are stricter than HIPAA, creating compliance complexity when integrating such data into a CPP (Yaqoob et al., 2022). The European Union's General Data Protection Regulation (GDPR) offers stronger individual rights (access, erasure, portability) and bases processing on lawful grounds, but its interaction with clinical care contexts remains challenging to implement (Mohammad Amini et al., 2023). Figure 1 illustrates the conceptual architecture of the Centralized Patient Profile (CPP), showing the integration of heterogeneous data domains, including clinical narratives, epidemiological risk factors, genetic and laboratory data, and administrative information.

Table 1: Ethical and Legal Challenges of Specific Data Types in a CPP

Data Type	Source Discipline	Primary Ethical Risks	Governing Legal Framework(s)	Key Regulatory Gaps
Nursing Narrative Notes	Nursing	Stigmatization, violation of therapeutic alliance, bias in care.	HIPAA, State Laws.	No special protection for psychotherapy notes' equivalent in nursing; highly subjective data is broadly accessible.
Epidemiological Risk Factors (Travel, Occupation)	Public Health/Epidemiology	Discrimination (employment, insurance), social stigma, privacy intrusion.	HIPAA, minimal specific protection.	Often considered less sensitive, but highly revealing in aggregate (e.g., links to political/sexual activity).
Genetic Test Results	Laboratory/Genomics	Familial implications, psychological harm, genetic discrimination beyond health.	HIPAA, GINA.	GINA does not cover life/disability insurance; "secondary findings" management is unclear in shared records.
Administrative/Billing Data	Medical Secretary/Admin	Financial privacy, exposure of diagnoses via codes, use for non-clinical purposes.	HIPAA.	Broad TPO allowance grants excessive access to clinical data for administrative staff.
Integrated Inferences	Informatics/Analytics	Inferred sensitive conditions, predictive profiling, loss of autonomy.	Largely unregulated.	No legal recognition or governance for data *inferred* from the CPP, only for what is directly entered.

Figure 1. Conceptual Architecture of the Centralized Patient Profile in Multidisciplinary Healthcare

The Disciplinary "Right to Know"

A fundamental challenge is defining what portion of the CPP each member of the care team needs to see to perform their role effectively and safely—their contextual "right to know."

Clinical Care Team

Clinicians traditionally assert a need for full access to provide safe care. However, evidence suggests information overload and the presence of sensitive "non-pertinent" information can actually impair clinical judgment and harm the therapeutic relationship (Blease et al., 2022). For example, a nurse's note expressing suspicion of non-adherence may bias a hospitalist's treatment decisions. The ethical question is whether the principle of beneficence always overrides patient privacy preferences for specific data elements (Caine & Tierney, 2015).

Epidemiologists may need population-level data or de-identified records for surveillance but rarely need identified, full-text clinical notes for individual cases. Their access should be tightly governed by public health purpose, not by default clinical permissions (Burris et al., 2016). While lab technicians need specific test orders and results, they do not typically require the full clinical narrative. However, for complex genomic interpretation, some clinical context may be necessary, creating a need for selective, purpose-driven data sharing (Clayton et al., 2019).

The access needs of administrative staff are largely non-clinical: scheduling, billing, and insurance verification. Their access to clinical narratives, psychotherapy notes, or genetic data is rarely justified by the principle of least privilege, yet it is routinely enabled (Brkić et al., 2023). This represents one of the most glaring failures in current access models.

Informatics Solutions from Role-Based to Context-Aware Access Control

Addressing these challenges requires technological sophistication beyond basic username/password logins. The evolution of access

control models is central to ethically managing the CPP (Table 2).

The Limitations of Role-Based Access Control (RBAC)

The predominant model, RBAC, grants permissions based on a user's role (e.g., "nurse," "physician," "coder"). This is too coarse-grained for the CPP. It fails to account for context (e.g., is this nurse the primary care nurse or covering in the ED?), sensitivity of data, or patient-specific consent directives (Hsieh, 2021). Under RBAC, a "physician" role often grants access to all data for all patients in the system, an obvious over-provision.

Towards Attribute-Based and Context-Aware Access Control (ABAC/CABAC)

More advanced models consider multiple attributes: the user (role, department, current task), the resource (data sensitivity, type), the environment (location, time of day), and the patient (consent directives) (Hu et al., 2014). A Context-Aware Access Control (CABAC) system could, for example, allow an emergency department physician to see a patient's psychiatric history only if the patient presents with an overdose, and even then, might mask specific therapist names per patient consent (Jin et al., 2009). These models enable the segmentation or "compartmentalization" of sensitive data within the shared record.

Data Segmentation and "Break-the-Glass" Protocols

Data segmentation involves tagging and isolating specific data elements (e.g., genetic results, STD diagnoses, substance use notes) so they can be protected with stricter access rules (Hermes et al., 2020). This must be paired with patient-mediated consent tools that allow individuals to express preferences for certain data segments. For emergencies, "break-the-glass" (BTG) protocols provide override access but create a mandatory, auditable trail for subsequent review (Zhang et al., 2021). The technical implementation of segmentation within legacy EHR architectures, however, remains a significant hurdle (Ancker et al., 2019).

Cryptographic and Privacy-Enhancing Technologies (PETs)

Emerging technologies offer promise. Homomorphic encryption allows computations on encrypted data without decryption, enabling research on CPP data without exposing individual records (Acar et al., 2018). Zero-knowledge proofs could allow a system to confirm a patient meets certain criteria (e.g., is over 18, has a specific diagnosis) without revealing the underlying data, facilitating eligibility checks without full disclosure (Dagher et al., 2018). Figure 2 depicts an ethical, privacy-by-design access control model for the Centralized Patient Profile.

Discussion

The Centralized Patient Profile must be reconceptualized not as a passive technical repository, but as a dynamic and potent representation of the patient's **digital self**. This construct demands a governing architecture that is fundamentally ethical in its design, operation, and governance (Mittelstadt & Floridi, 2016). The findings of this review converge on the necessity for a multi-layered approach to counter the inherent risks of aggregation, moving beyond technical fixes to address cultural, legal, and educational foundations.

Table 2: Evolution of Access Control Models for the Centralized Patient Profile

Model	Core Mechanism	Advantages	Disadvantages for CPP	Suitability for Multidisciplinary Care
Discretionary (DAC)	Data owner controls access.	Empowers patient autonomy.	Impractical in emergency care; patients lack expertise to manage.	Low - too complex and risky for clinical workflow.
Mandatory (MAC)	System-enforced labels (e.g., "Confidential").	Strong, uniform security policy.	Inflexible; cannot adapt to dynamic clinical contexts.	Low - too rigid for variable care needs.
Role-Based (RBAC)	Permissions tied to professional role.	Simple to administer, scalable.	Coarse-grained; allows excessive access; ignores context & consent.	Moderate (currently dominant) but ethically insufficient.
Attribute-Based (ABAC)	Policies evaluate user/resource/environment attributes.	Highly granular, flexible, enables fine-grained policies.	Policy management can be complex; performance overhead.	High - can balance need-to-know with privacy.
Context-Aware (CABAC)	Dynamic evaluation of real-time context.	Most granular, respects situational need.	Technically complex to implement; requires rich metadata.	Very High - ideal for ethical, just-in-time data sharing.

Saudi Journal of Medicine and Public Health

ijmph.com/index.php/pub
rg/10.64483/202412517

Figure 2. Context-Aware Access Control and Ethical Data Segmentation in the Centralized Patient Profile

A foundational and non-negotiable imperative is a **paradigm shift in clinical culture and system design**, from the prevailing norm of "all data to all clinicians" to a disciplined practice of sharing "minimum necessary data in context." This requires the operational fusion of the core ethical principle of **respect for persons** with the cybersecurity axiom of **least privilege** (Mittelstadt, 2019). Embedding this into EHR design means that access is not a default right of role, but a contextually granted privilege. Consequently, a parallel cultural shift is required among healthcare professionals, who must come to view the respectful segmentation of sensitive information not as a bureaucratic obstacle to care, but as an integral component of patient autonomy and professional integrity (Caine & Tierney, 2015; Blease et al., 2022). Failing to make this shift perpetuates systemic privacy violations under the guise of clinical necessity.

Translating this principle into practice necessitates the rigorous implementation of **Privacy by Design (PbD)** as the core methodology for CPP development. PbD's tenets—proactivity, embeddedness, and user-centricity—must be engineered into the data lifecycle from its origin (Cavoukian, 2009). This means that sensitivity and intended use are evaluated at the point of data entry, not applied as a retrospective filter. For example, a structured data field could require a clinician documenting a mental health assessment or a social determinant of health to assign a sensitivity classification from a standardized ontology (e.g., "psychiatric," "substance use," "genetic"), which would then automatically enforce predefined, granular access rules (Hermes et al., 2020). This proactive, metadata-driven approach ensures privacy controls are intrinsic, dynamic, and travel with the data element throughout its existence within the aggregated profile.

However, an ethical architecture cannot be imposed paternalistically; it requires the **active engagement of patients as stewards of their own digital identity**. This mandates a significant evolution of patient portals from passive viewing windows into interactive control panels. Patients should be empowered through usable interfaces to set granular privacy preferences for different data categories, review transparent access audit logs (a fully functional "who viewed my record" report), and receive clear explanations of how their aggregated data is utilized for secondary purposes like research or operational analytics (Zaidi et al., 2022; Avdagovska et al., 2020). Such **radical transparency** is not merely a feature but a prerequisite for restoring meaningful autonomy and fostering trust, enabling patients to participate in the governance of their digital selves (Ploug & Holm, 2015).

Ultimately, these technical and cultural advancements will falter without supportive **policy reform and interdisciplinary education**. Existing legal frameworks, particularly the U.S. Health Insurance Portability and Accountability Act (HIPAA), are demonstrably inadequate for governing the modern CPP. Legislative action is needed to strengthen HIPAA by mandating technical support for fine-grained data segmentation and by critically narrowing the overly broad "Treatment, Payment, and Operations" (TPO) provision that currently justifies excessive access to highly sensitive data segments by non-clinical personnel (Price & Cohen, 2019; Cohen & Mello, 2018). Concurrently, a mandatory, interdisciplinary curriculum for all healthcare staff is essential. This education must cover the ethical nuances of information sharing, the mitigation of implicit bias that can be triggered by exposure to stigmatizing data, and the responsible navigation of the powerful CPP within a team-based care model (Avdagovska et al., 2020; Hornum et al., 2023). Only through this concerted, multi-pronged strategy—synthesizing ethical design, empowered patients, updated law, and renewed professional formation—can a truly ethical architecture for the digital self be realized.

Conclusion

The Centralized Patient Profile represents both the apex of health informatics aspiration and a nexus of profound ethical, legal, and security challenges. This review has demonstrated that the risks are not ancillary but are intrinsic to its power: harms of aggregation, discriminatory misuse, and the erosion of autonomy are amplified by integration. Current legal frameworks, built for a siloed era, are woefully inadequate. While Role-Based Access Control remains the operational norm, it is ethically bankrupt for governing the multidisciplinary use of such rich profiles.

The path forward requires a deliberate and collaborative effort. Technologists must prioritize the development and implementation of sophisticated, context-aware access models and segmentation tools that are clinically usable. Clinicians and administrators must embrace a culture of data

*Corresponding author e-mail: Faishi@moh.gov.sa (Fadiyah Ali Ayishi).
Receive Date: 20 December 2024, Revise Date: 30 December 2024, Accept Date: 31 December 2024

minimalism and vigilant stewardship. Policymakers must craft laws that recognize the unique sensitivity of aggregated health data and provide meaningful protections and rights. Ultimately, the goal must be to build ethical systems—CPPs that are not just repositories of information, but architectures of trust that safeguard the digital self while enabling the collective endeavor of healing. The integrity of the multidisciplinary healthcare project in the digital age depends on it.

References

1. Acar, A., Aksu, H., Uluagac, A. S., & Conti, M. (2018). A survey on homomorphic encryption schemes: Theory and implementation. *ACM Computing Surveys (Csur)*, *51*(4), 1-35. https://doi.org/10.1145/3214303
2. Adler-milstein, J., & Pfeifer, E. (2017). Information blocking: is it occurring and what policy strategies can address it?. *The Milbank Quarterly*, *95*(1), 117-135. https://doi.org/10.1111/1468-0009.12247
3. Ancker, J. S., Edwards, A. M., Miller, M. C., & Kaushal, R. (2012). Consumer perceptions of electronic health information exchange. *American journal of preventive medicine*, *43*(1), 76-80. https://doi.org/10.1016/j.amepre.2012.02.027
4. Avdagovska, M., Menon, D., & Stafinski, T. (2020). Capturing the impact of patient portals based on the quadruple aim and benefits evaluation frameworks: scoping review. *Journal of medical Internet research*, *22*(12), e24568. https://doi.org/10.2196/24568
5. Blease, C., Salmi, L., Rexhepi, H., Hägglund, M., & DesRoches, C. M. (2022). Patients, clinicians and open notes: information blocking as a case of epistemic injustice. *Journal of Medical Ethics*, *48*(10), 785-793. https://doi.org/10.1136/medethics-2021-107275
6. Brkić, M., Dinu, H. S., Mirković, A., Sabirović, A., Khan, S., & Svetinović, D. (2023, November). Cyber Vulnerabilities in Blockchain Electronic Health Records: An In-Depth Threat Analysis. In *2023 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)* (pp. 0784-0791). IEEE. https://doi.org/10.1109/DASC/PiCom/CBDCom/Cy59711.2023.10361458
7. Burris, S., Ashe, M., Levin, D., Penn, M., & Larkin, M. (2016). A transdisciplinary approach to public health law: the emerging practice of legal epidemiology. *Annual review of public health*, *37*(1), 135-148. https://doi.org/10.1146/annurev-publhealth-032315-021841
8. Caine, K., & Tierney, W. M. (2015). Point and counterpoint: patient control of access to data in their electronic health records. *Journal of general internal medicine*, *30*(Suppl 1), 38-41. https://doi.org/10.1007/s11606-014-3061-0
9. Cavoukian, A. (2009). Privacy by design: The 7 foundational principles. *Information and privacy commissioner of Ontario, Canada*, *5*(2009), 12.
10. Childress, J. F., & Beauchamp, T. L. (2022). Common morality principles in biomedical ethics: responses to critics. *Cambridge Quarterly of Healthcare Ethics*, *31*(2), 164-176. doi:10.1017/S0963180121000566
11. Clayton, E. W., Evans, B. J., Hazel, J. W., & Rothstein, M. A. (2019). The law of genetic privacy: applications, implications, and limitations. *Journal of Law and the Biosciences*, *6*(1), 1-36. https://doi.org/10.1093/jlb/lsz007
12. Cohen, I. G. (2019). Informed consent and medical artificial intelligence: what to tell the patient?. *Geo. LJ*, *108*, 1425.
13. Cohen, I. G., & Mello, M. M. (2018). HIPAA and protecting health information in the 21st century. *Jama*, *320*(3), 231-232. doi:10.1001/jama.2018.5630
14. Dagher, G. G., Mohler, J., Milojkovic, M., & Marella, P. B. (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustainable cities and society*, *39*, 283-297. https://doi.org/10.1016/j.scs.2018.02.014
15. Hermes, S., Riasanow, T., Clemons, E. K., Böhm, M., & Krcmar, H. (2020). The digital transformation of the healthcare industry: exploring the rise of emerging platform ecosystems and their influence on the role of patients. *Business Research*, *13*(3), 1033-1069. https://doi.org/10.1007/s40685-020-00125-x
16. Hornum, M. S., Steinsbekk, A., & Nøst, T. H. (2023). Views on patient portal use for adolescents in mental health care-a qualitative study. *BMC Health Services Research*, *23*(1), 132. https://doi.org/10.1186/s12913-023-09156-6
17. Hsieh, F. S. (2021). A dynamic context-aware workflow management scheme for cyber-physical systems based on multi-agent system architecture. *Applied Sciences*, *11*(5), 2030. https://doi.org/10.3390/app11052030
18. Hu, V. C., Ferraiolo, D., Kuhn, R., Schnitzer, A., Sandlin, K., Miller, R., &

Scarfone, K. (2014). Guide to attribute based access control (ABAC) definition and considerations. *NIST special publication*, *800*(162), 1-54.

19. Jin, J., Ahn, G. J., Hu, H., Covington, M. J., & Zhang, X. (2009, June). Patient-centric authorization framework for sharing electronic health records. In *Proceedings of the 14th ACM symposium on Access control models and technologies* (pp. 125-134). https://doi.org/10.1145/1542207.1542228
20. Keshta, I., & Odeh, A. (2021). Security and privacy of electronic health records: Concerns and challenges. *Egyptian Informatics Journal*, *22*(2), 177-183.https://doi.org/10.1016/j.eij.2020.07.003
21. Lenartz, A., Scherer, A. M., Uhlmann, W. R., Suter, S. M., Hartley, C. A., & Prince, A. E. (2021). The persistent lack of knowledge and misunderstanding of the Genetic Information Nondiscrimination Act (GINA) more than a decade after passage. *Genetics in Medicine*, *23*(12), 2324-2334. https://doi.org/10.1038/s41436-021-01268-w
22. Mittelstadt, B. (2019). The ethics of biomedical 'big data'analytics. *Philosophy & Technology*, *32*(1), 17-21.https://doi.org/10.1007/s13347-019-00344-z
23. Mittelstadt, B. D., & Floridi, L. (2016). The ethics of big data: current and foreseeable issues in biomedical contexts. *The ethics of biomedical big data*, 445-480. https://doi.org/10.1007/978-3-319-33525-4_19
24. Mohammad Amini, M., Jesus, M., Fanaei Sheikholeslami, D., Alves, P., Hassanzadeh Benam, A., & Hariri, F. (2023). Artificial intelligence ethics and challenges in healthcare applications: a comprehensive review in the context of the European GDPR mandate. *Machine Learning and Knowledge Extraction*, *5*(3), 1023-1035. https://doi.org/10.3390/make5030053
25. Obermeyer, Z., Powers, B., Vogeli, C., & Mullainathan, S. (2019). Dissecting racial bias in an algorithm used to manage the health of populations. *Science*, *366*(6464), 447-453. https://doi.org/10.1126/science.aax2342
26. Ploug, T., & Holm, S. (2015). Meta consent: a flexible and autonomous way of obtaining informed consent for secondary research. *Bmj*, *350*. https://doi.org/10.1136/bmj.h2146
27. Price, W. N., & Cohen, I. G. (2019). Privacy in the age of medical big data. *Nature medicine*, *25*(1), 37-43. https://doi.org/10.1038/s41591-018-0272-7
28. Prince, A. E., & Roche, M. I. (2014). Genetic information, non-discrimination, and privacy protections in genetic counseling practice. *Journal of genetic counseling*, *23*(6), 891-902. https://doi.org/10.1007/s10897-014-9743-2
29. 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. https://doi.org/10.1038/s41467-019-10933-3
30. Rothstein, M. A. (2016). The end of the HIPAA privacy rule? Currents in contemporary bioethics. *The Journal of Law, Medicine & Ethics*, *44*(2), 352-358. https://doi.org/10.1177/1073110516654128
31. Shaban-Nejad, A., Michalowski, M., & Buckeridge, D. L. (2018). Health intelligence: how artificial intelligence transforms population and personalized health. *NPJ digital medicine*, *1*(1), 53. https://doi.org/10.1038/s41746-018-0058-9
32. Shahid, J., Ahmad, R., Kiani, A. K., Ahmad, T., Saeed, S., & Almuhaideb, A. M. (2022). Data protection and privacy of the internet of healthcare things (IoHTs). *Applied Sciences*, *12*(4), 1927. https://doi.org/10.3390/app12041927
33. Staunton, C., Slokenberga, S., & Mascalzoni, D. (2019). The GDPR and the research exemption: considerations on the necessary safeguards for research biobanks. *European Journal of Human Genetics*, *27*(8), 1159-1167. https://doi.org/10.1038/s41431-019-0386-5
34. Veinot, T. C., Mitchell, H., & Ancker, J. S. (2018). Good intentions are not enough: how informatics interventions can worsen inequality. *Journal of the American Medical Informatics Association*, *25*(8), 1080-1088.
35. Yaqoob, I., Salah, K., Jayaraman, R., & Al-Hammadi, Y. (2022). Blockchain for healthcare data management: opportunities, challenges, and future recommendations. *Neural Computing and Applications*, *34*(14), 11475-11490. https://doi.org/10.1007/s00521-020-05519-w
36. Zhang, R., Liu, G., Kang, H., Wang, Q., Tian, Y., & Wang, C. (2021). Improved Bell–LaPadula model with break the glass mechanism. *IEEE Transactions on Reliability*, *70*(3), 1232-1241. https://doi.org/10.1109/TR.2020.3046768
37. Zaidi, M., Amante, D. J., Anderson, E., Ito Fukunaga, M., Faro, J. M., Frisard, C., ... & Lemon, S. C. (2022). Association between patient portal use and perceived patient-centered communication among adults with

cancer: cross-sectional survey study. *JMIR cancer*, *8*(3), e34745. https://doi.org/10.2196/34745

.