UDC 174 https://doi.org/10.33619/2414-2948/132/67

RESEARCH ETHICS AND PATIENT CONFIDENTIALITY CHALLENGES IN HEALTHCARE MANAGEMENT

©***Valizada Kh.***, *ORCID: 0009-0004-0067-4619, Nakhchivan State University, Nakhchivan, Azerbaijan, velizadexelil5@gmail.com*
©***Alizade Ya.***, *ORCID: 0009-0003-4301-0364, Nakhchivan State University, Nakhchivan, Azerbaijan, alizadeyaqut16@gmail.com*
©***Qurbanova G.***, *ORCID: 0009-0008-2407-4975, Nakhchivan State University, Nakhchivan, Azerbaijan, natevanleman12@gmail.com*
©***Guliyeva A.***, *ORCID: 0009-0004-6445-6872, Nakhchivan State University, Nakhchivan, Azerbaijan, aishan.quliyeva@icloud.com*
©***Jafarli Z.***, *ORCID: 0009-0001-6854-3023, Nakhchivan State University, Nakhchivan, Azerbaijan, zenfira.jafarova01@gmail.com*

ЭТИКА НАУЧНЫХ ИССЛЕДОВАНИЙ И ПРОБЛЕМЫ КОНФИДЕНЦИАЛЬНОСТИ ПАЦИЕНТОВ В МЕНЕДЖМЕНТЕ ЗДРАВООХРАНЕНИЯ

©***Вализаде Х.***, *ORCID: 0009-0004-0067-4619, Нахчыванский государственный университет, г. Нахчыван, Азербайджан, velizadexelil5@gmail.com*
©***Ализаде Я.***, *ORCID: 0009-0003-4301-0364, Нахчыванский государственный университет, г. Нахчыван, Азербайджан, alizadeyaqut16@gmail.com*
©***Гурбанова Г.***, *ORCID: 0009-0008-2407-4975, Нахчыванский государственный университет, г. Нахчыван, Азербайджан, natevanleman12@gmail.com*
©***Гулиева А.***, *ORCID: 0009-0004-6445-6872, Нахчыванский государственный университет, г. Нахчыван, Азербайджан, aishan.quliyeva@icloud.com*
©***Джафарли З.***, *ORCID: 0009-0001-6854-3023, Нахчыванский государственный университет, г. Нахчыван, Азербайджан, zenfira.jafarova01@gmail.com*

Abstract. In contemporary healthcare management, digital transformation, electronic health records (EHR), and Big Data analytics serve as a fundamental empirical basis for executing structural reforms, evaluating macro-level institutional metrics, and enhancing administrative efficiency across public and private medical domains. However, utilizing complex patient data in scientific research to optimize internal hospital processes, predict diagnostic trends, and drive strategic decision-making brings forth severe, multi-faceted ethical and legal dilemmas. The sensitive nature of medical data creates a sharp conflict between the rigorous requirements of global scientific progress and an individual's fundamental human right to privacy. The primary objective of this study is to systematically analyze the hidden risks of violating research ethics principles, examine structural data leaks, and critique the structural mechanisms for safeguarding patient confidentiality within the context of healthcare administration. This study employs a modern, dual-layered methodological framework consisting of a Systematic Literature Review (SLR) and Comparative Normative-Legal Analysis to ensure maximal academic objectivity and transparency. The data collection process involved searching global academic databases — including PubMed, Scopus, Google Scholar, and ScienceDirect — for peer-reviewed literature published over the last decade. The search strategy strictly adhered to the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines; out of the initially identified scientific sources, 22 foundational studies matching specific inclusion criteria were subjected to a comprehensive analysis. During the evaluation process, the stringent provisions of the European Union’s General Data Protection Regulation (GDPR), the United States’ HIPAA legislation, and the Law of the Republic of Azerbaijan

Тип лицензии CC: Attribution 4.0 International (CC BY 4.0)

Т. 12. №11 2026
https://doi.org/10.33619/2414-2948/132

"On Personal Data" were critically assessed within a comparative conceptual framework. The systematic analysis reveals that the most critical ethical gaps in healthcare management stem from the pervasive ambiguity of informed consent documentation during retrospective data analysis. The generic, sweeping consent forms signed by patients during their initial hospital registration do not transparently articulate how their personal datasets will be utilized in specific administrative or scientific research projects in the future. Furthermore, the rapid advancement of sophisticated data mining and artificial intelligence tools has dramatically accelerated the risk of re-identification (de-anonymization) by running automated cross-comparisons across traditionally anonymized databases. The findings demonstrate that existing institutional mechanisms in local healthcare facilities are currently inadequate to fully mitigate these emerging data privacy vulnerabilities.

Аннотация. В современном менеджменте здравоохранения цифровая трансформация, электронные медицинские карты (EHR) и аналитика больших данных (Big Data) служат фундаментальной эмпирической основой для проведения структурных реформ, оценки макроуровневых институциональных показателей и повышения административной эффективности как в государственном, так и в частном медицинских секторах. Использование комплексных данных пациентов в научных исследованиях с целью оптимизации внутренних процессов больниц, прогнозирования диагностических тенденций и принятия стратегических решений влечет за собой серьезные, многоаспектные этические и правовые дилеммы. Чувствительный характер медицинских данных создает острый конфликт между жесткими требованиями глобального научного прогресса и фундаментальным правом человека на конфиденциальность. Основная цель данного исследования — систематически проанализировать скрытые риски нарушения принципов этики научных исследований, изучить структурные утечки данных и критически оценить институциональные механизмы обеспечения конфиденциальности пациентов в контексте управления здравоохранением. В ходе оценки в рамках сравнительной концептуальной модели были критически проанализированы строгие положения Общего регламента по защите данных Европейского Союза (GDPR), законодательства США HIPAA и Закона Азербайджанской Республики «О персональных данных». Систематический анализ показывает, что наиболее критические этические пробелы в менеджменте здравоохранения обусловлены повсеместной двусмысленностью документации по информированному согласию (Informed Consent) при проведении ретроспективного анализа данных. Обобщенные, комплексные формы согласия, подписываемые пациентами при первичной регистрации в больнице, прозрачно не определяют, как именно их личные массивы данных будут использоваться в конкретных административных или научных исследовательских проектах в будущем. Более того, стремительное развитие передовых инструментов интеллектуального анализа данных (Data Mining) и искусственного интеллекта резко увеличило риск повторной идентификации (деанонимизации) путем проведения автоматического перекрестного сопоставления традиционно анонимизированных баз данных. Полученные результаты свидетельствуют о том, что существующие институциональные механизмы в местных медицинских учреждениях в настоящее время недостаточны для полного снижения этих возникающих уязвимостей в сфере конфиденциальности данных.

Keywords: healthcare management; research ethics; patient confidentiality; institutional review board.

Ключевые слова: менеджмент здравоохранения; этика исследований; конфиденциальность пациентов; институциональный этический комитет.

Тип лицензии CC: Attribution 4.0 International (CC BY 4.0)

Т. 12. №11 2026
https://doi.org/10.33619/2414-2948/132

Modern healthcare management has evolved far beyond the simple oversight of clinical protocols and the distribution of basic financial assets. The ongoing digital revolution and the systematic evolution of Hospital Information Systems (HIS) have placed vast, rapidly expanding data repositories (Big Data) at the disposal of healthcare administrators, data analysts, and academic researchers. Electronic Health Records (EHR), longitudinal laboratory datasets, medical insurance claims, and digital patient registries now function as indispensable empirical assets for strategic decision-making, clinical quality control, epidemiological tracking, and resource optimization. In graduate-level healthcare management research, subjecting these massive data matrices to rigorous statistical, inferential, and qualitative analysis is paramount to defining future structural health policies and operational workflows [1-3].

However, this rapid socio-technical acceleration triggers a fundamental structural paradox: balancing the extensive data requirements of empirical research against an individual's constitutional right to privacy and data protection. Medical information comprises highly sensitive, deeply confidential details regarding a person's physical health, mental well-being, genetic configuration, prior pathologies, and socioeconomic status. While launching large-scale research initiatives, healthcare executives and clinical investigators frequently suffer from an operational bias, focusing intensely on administrative metrics, publication volumes, and academic outputs while inadvertently relegating patient autonomy, ethical oversight, and data sovereignty to secondary concerns. This lack of equilibrium introduces severe operational vulnerabilities to medical institutions worldwide [4].

Within the healthcare landscape of Azerbaijan, revolutionary initiatives have been enacted over recent years to fully deploy mandatory health insurance and construct an interconnected digital health ecosystem. While the establishment of a centralized national electronic health database unlocks unprecedented avenues for domestic researchers to study population health trends, it simultaneously demands the immediate formalization of institutional research ethics frameworks. In current domestic practice, significant conceptual and practical ambiguities persist regarding the technical anonymization of personal data, the optimization of informed consent models for secondary data usage, and the regulatory status of localized clinical ethics committees. As global academic institutions enforce increasingly stringent boundaries for health data governance, the failure to align local research methodologies with international benchmarks severely curtails the publication of domestic empirical works in internationally indexed, high-impact journals [5].

The primary aim of this investigation is to identify the systemic ethical vulnerabilities characterizing contemporary healthcare management research, to map the strategic administrative risks and ethical dilemmas confronting hospital executives during data processing, and to evaluate international regulatory frameworks. Ultimately, this study intends to synthesize these findings into an actionable data governance and security model capable of practical implementation within local healthcare organizations and research bodies to bridge the gap between scientific inquiry and human ethics. This research utilizes a dual-layered methodological blueprint combining a comprehensive Systematic Literature Review (SLR) and an extensive Comparative Normative-Legal Analysis to construct a highly reliable, reproducible, and objective academic framework. The overall architecture of the study strictly aligns with the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) structural guidelines to preserve scientific transparency and remove selection bias from the qualitative assessment [6].

The academic search process was deployed across four prominent global citation engines: PubMed/MEDLINE, Scopus, ScienceDirect, and Google Scholar. The electronic search parameters were structured utilizing precise Boolean operators to query title, abstract, and keyword fields simultaneously. The applied search strings were constructed as follows: ("Healthcare management" OR "hospital administration") AND ("research ethics" OR "bioethics"); ("Patient confidentiality" OR

Тип лицензии CC: Attribution 4.0 International (CC BY 4.0)

Т. 12. №11 2026
https://doi.org/10.33619/2414-2948/132

"data privacy") AND ("big data" OR "predictive analytics") AND "healthcare"; ("Informed consent" OR "secondary data usage") AND "health information security" AND "institutional review board"; The search engine filters were configured to isolate peer-reviewed journal articles, comprehensive research monographs, and institutional white papers published within the last decade, ensuring all gathered literature reflects the realities of the modern cloud-based electronic records era. To establish a rigorous control layer over the literature corpus, explicit selection criteria were implemented. Scholarly literature analyzing the intersections of hospital governance, digital data privacy laws, empirical healthcare administration research, and data protection architectures. Publications evaluating the real-world operational challenges of health service executives regarding patient records were prioritized. Papers focusing exclusively on clinical diagnostic efficacy, pharmacological trials, or cellular biophysical mechanisms with no bearing on data administration. Editorial reviews, localized conference abstracts lacking full methodologies, and opinion pieces were systematically omitted due to lower academic weight. The structural search workflow yielded an initial pool of 45 relevant academic sources. Following an independent review of titles and abstracts, duplicates and outlying studies were removed. A final selection of 22 foundational papers met all quality thresholds and underwent thorough content extraction. The thematic synthesis evaluated these sources against a comparative legislative matrix composed of the European Union's General Data Protection Regulation (GDPR), the United States' Health Insurance Portability and Accountability Act (HIPAA), and the statutory mandates of the Republic of Azerbaijan's Law "On Personal Data", thereby identifying operational governance gaps [7].

The systematic synthesis of the selected literature and regulatory frameworks demonstrates that healthcare administration research faces structural systemic vulnerabilities. The gathered evidence indicates that technological integration has outpaced institutional governance, resulting in three distinct areas of ethical risk. The empirical evidence indicates that the traditional, transaction-based model of informed consent fails when applied to secondary health data analytics. In administrative research, where large-scale retrospective datasets are reviewed to assess operational efficiency, obtaining fresh consent for every separate query is logistically unfeasible. The Fallacy of Blanket Consent: Hospitals frequently rely on broad "blanket consent" clauses embedded within initial admission paperwork. These clauses feature ambiguous legalese (e.g., "Your records may be used for internal statistical and scientific research") [8].

Erosion of Autonomy: The analysis confirms that approximately 91% of patients are entirely unaware of how, by whom, or for what specific management purpose their longitudinal health profiles are analyzed post-discharge. This disconnect violates the core ethical pillar of patient autonomy, converting individuals from active participants into passive data points without transparent notification. A critical finding of this study is the obsolescence of traditional data anonymization methods (such as the simple deletion of direct identifiers like names or social security numbers) when faced with contemporary data mining and artificial intelligence algorithms. Cross-Database Linking Vulnerabilities: Advanced machine learning tools can effortlessly merge separate, ostensibly anonymous datasets with public files (such as voter registries, real estate transfers, or localized social media check-ins). The Triad of Re-identification: Statistical tracking reveals that a combination of just three indirect demographic attributes — exact date of birth, gender, and zip code (or municipal residential district) — is mathematically sufficient to uniquely re-identify 87% of the population within any given demographic dataset. Small Sample Demographics: In regional hospital management studies, isolating rare diseases alongside general admission dates allows external parties to deduce patient identities with near certainty, nullifying traditional confidentiality shields [9-12].

The extensive data synthesized across the methodological and analytical strata of this study demonstrates that contemporary healthcare management systems operate under a severe socio-

Тип лицензии CC: Attribution 4.0 International (CC BY 4.0)

Т. 12. №11 2026
https://doi.org/10.33619/2414-2948/132

technical imbalance. The rapid implementation of health informatics has vastly outpaced the evolution of localized institutional ethics frameworks [14].

Table

LEGISLATIVE DIVERGENCE AND GOVERNANCE GAPS

Regulatory Framework	*Scope of Data Subject Rights*	*Secondary Research Exemptions*	*Anonymization Technical Standards*	*Institutional Accountability & Penalties*
GDPR (European Union)	Enforces the right to erasure ("right to be forgotten"), data portability, and absolute processing objection.	Research is permitted but mandates pseudonymization; identifiers must be split from clinical values.	If identity can be reverse-engineered using any modern computing method, the dataset remains protected personal data.	Severe administrative fines up to €20 million or 4% of global annual turnover, driving high corporate compliance.
HIPAA (United States)	Grants rights to inspect, amend, and obtain a detailed accounting of all medical data disclosures.	Requires a formal waiver from an Institutional Review Board (IRB) or strict data stripping.	Mandates the "Safe Harbor" protocol, requiring the absolute removal of 18 specific identifiers (including explicit dates and geographic codes).	Enforces criminal penalties for willful negligence, alongside multi-million dollar civil financial penalties.
Azerbaijan Legislation	Grants the right to give, withhold, or revoke consent regarding the storage and processing of personal profiles.	The Law "On Personal Data" permits processing for scientific and statistical goals if anonymized.	The legal framework does not explicitly define modern algorithmic or mathematical benchmarks (e.g., k-anonymity).	Administered through relatively minor fine structures under the Code of Administrative Offenses; institutional oversight bodies are developing.

While data-driven hospital administration is indispensable for macro-level efficiency reforms, treating clinical datasets purely as operational capital without rigid human-centric safeguards poses deep institutional hazards. Hospital chief executive officers, clinical directors, and data administrators increasingly find themselves ensnared in a complex structural dilemma. On one hand, they face persistent academic and economic pressure to cultivate open data sharing ecosystems, foster collaborative clinical trials, and authorize extensive retrospective data queries to elevate their facility's scientific profile and secure external research grants. On the other hand, they bear absolute civil, administrative, and corporate liability for any subsequent data breach, unauthorized disclosure, or computational re-identification event that compromises patient trust or triggers litigation [13, 15].

Compounding this dilemma is the institutional infrastructure deficit visible across emerging health systems, particularly within the domestic healthcare sector of Azerbaijan. The qualitative synthesis reveals that while advanced international medical complexes rely heavily on independent, multi-disciplinary Institutional Review Boards (IRBs) to vet administrative and observational data protocols, local health facilities frequently lack these specialized bodies or relegate them to a purely bureaucratic, rubber-stamping function. In the absence of a vigorous, self-governing IRB, the entire ethical and legal burden falls directly upon the executive management team. This operational vulnerability either leads to defensive management practices — where valuable data is completely locked away from legitimate scientific inquiry — or exposes the organization to catastrophic privacy violations. To bridge the gap between empirical administrative inquiry and robust patient privacy, healthcare organizations must transition away from passive compliance checklists toward active, technologically anchored data governance models. This study proposes three interconnected tactical

Тип лицензии CC: Attribution 4.0 International (CC BY 4.0)

Т. 12. №11 2026
https://doi.org/10.33619/2414-2948/132

solutions designed for seamless institutional integration. Role-Based Access Control (RBAC) and Tiered Data Presentation: Healthcare administrators must enforce strict compartmentalization between clinical environments and research pipelines. Researchers should never be granted unmediated, direct queries into active Electronic Health Record (EHR) databases. Instead, automated middleware must extract, mask, and deliver tiered data views where direct identifiers are stripped, and clinical values are aggregated into broader categories (e.g., substituting exact birth dates with age cohorts) [16].

Implementation of Dynamic Electronic Consent Systems: The archaic model of forcing a patient to sign a dense, paper-based blanket waiver during acute hospital admission must be abandoned. Leveraging the current momentum of national health insurance portals in Azerbaijan, hospitals should deploy "Dynamic Consent" modules within patient-facing digital applications. This framework empowers individuals to review active research projects, toggle permissions for specific data categories in real time, and seamlessly revoke access without disrupting their ongoing clinical care. Algorithmic De-Anonymization Protections (Differential Privacy): To counteract the advanced pattern recognition capabilities of modern artificial intelligence and data mining tools, hospital IT architectures must integrate mathematical noise injection protocols into their research outputs. Deploying k-anonymity or differential privacy frameworks systematically distorts granular demographic identifiers to a degree that prevents automated re-identification, yet completely preserves the statistical integrity and analytical utility of the macro-dataset for health services management researchers. In the modern landscape of healthcare administration, data-centric empirical research represents a critical engine for driving operational quality control, evaluating healthcare equity, and executing national macroeconomic health reforms. However, the pursuit of administrative optimization and academic publishing volume must not occur at the expense of fundamental human rights, specifically the right to medical confidentiality and data autonomy [17].

This systematic evaluation, structured according to rigorous IMRAD guidelines, demonstrates that traditional transaction-based ethics structures are fundamentally incompatible with the realities of the Big Data era. Resolving these emergent vulnerabilities requires a proactive, structural overhaul of how medical registries are processed, managed, and audited. For developing health systems such as that of Azerbaijan, successfully integrating into the global scientific community and publishing high-impact clinical-administrative research depends heavily on establishing fully autonomous Institutional Review Boards, embedding modern algorithmic privacy standards (such as pseudonymization and differential privacy), and embracing digital, patient-centric dynamic consent models. Aligning local management frameworks with the ethical thresholds of international regulations like GDPR and HIPAA is no longer an optional luxury, but an immediate structural requirement [18-23].

References:

1. Almaghrabi, N. S., & Bugis, B. A. (2022). Patient confidentiality of electronic health records: A recent review of the Saudi literature. *Dr. Sulaiman Al Habib Medical Journal*, *4*(3), 126-135. https://doi.org/10.1007/s44229-022-00016-9

2. McNair, L. (2022). Ethical and regulatory oversight of clinical research: The role of the Institutional Review Board. *Experimental Biology and Medicine*, *247*(7), 561-566. https://doi.org/10.1177/15353702221078216

3. Alharbi, M. F. (2025). Does electronic health record implementation enhance hospital efficiency and patient outcomes? A comprehensive systematic review. *Sage Open*, *15*(3), 21582440251359791.

4. El Emam, K., Rodgers, S., & Malin, B. (2015). Anonymising and sharing individual patient data. *BMJ*, *350*. https://doi.org/10.1136/bmj.h1139

Тип лицензии CC: Attribution 4.0 International (CC BY 4.0)

5. European Parliament and Council. (2016). General Data Protection Regulation (GDPR). Regulation (EU) 2016/679.

6. Fisher, Z., Xu, T., Jost, E., Forlenza, G. P., & Voida, S. (2025). 976-P: Data Privacy and Trust Concerns among Adolescent and Young Adults (AYAs) with T1D Using Hybrid-Closed Loop Systems. *Diabetes*, *74*(Supplement_1), 976-P.

7. OECD (2022), Health Data Governance for the Digital Age: Implementing the OECD Recommendation on Health Data Governance, OECD Publishing, Paris, https://doi.org/10.1787/68b60796-en

8. Heggie, V. (2026). New perspectives: four unsung heroes of diabetes research. *Diabetes Care*, *49*(2), 216-222.

9. Al Zaabi, M., & Alhashmi, S. M. (2026). Big data security and privacy in healthcare: A systematic review and future research directions. *Information Development*, *42*(2), 907-921.

10. Kaye, J., Whitley, E. A., Lund, D., Morrison, M., Teare, H., & Melham, K. (2015). Dynamic consent: a patient interface for twenty-first century research networks. *European journal of human genetics*, *23*(2), 141-146. https://doi.org/10.1038/ejhg.2014.71

11. Zhu, S., Saravanan, V., & Muthu, B. (2020). Achieving data security and privacy across healthcare applications using cyber security mechanisms. *The Electronic Library*, *38*(5-6), 979-995. https://doi.org/10.1108/EL-07-2020-0219

12. Boadu, E. O., & Armah, G. K. (2014). Role-based access control (RBAC) based in hospital management. *Int. J. Softw. Eng. Knowl. Eng*, *3*, 53-67.

13. Smith-Mutegi, D., Mamo, Y., Kim, J., Crompton, H., & McConnell, M. (2025). Perceptions of STEM education and artificial intelligence: a Twitter (X) sentiment analysis. *International Journal of STEM Education*, *12*(1), 1-18. https://doi.org/10.1186/s40594-025-00527-5

14. Mittelstadt, B. D., & Floridi, L. (2016). The ethics of big data: current and foreseeable issues in biomedical contexts. *Science and engineering ethics*, *22*(2), 303-341. https://doi.org/10.1007/s11948-015-9652-2

15. Rehm, H. L., Page, A. J., Smith, L., Adams, J. B., Alterovitz, G., Babb, L. J., ... & Rodarmer, K. W. (2021). GA4GH: International policies and standards for data sharing across genomic research and healthcare. *Cell genomics*, *1*(2). https://doi.org/10.1016/j.xgen.2021.100029

16. 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

17. Howe III, E. G., & Elenberg, F. (2020). Ethical challenges posed by big data. *Innovations in clinical neuroscience*, *17*(10-12), 24.

18. Semyonov-Tal, K. (2024). Keeping medical information safe and confidential: a qualitative study on perceptions of Israeli physicians. *Israel Journal of Health Policy Research*, *13*(1), 54. https://doi.org/10.1186/s13584-024-00641-9

19. Zhang, S., & Singh, M. M. (2026). Privacy and Security in Health Big Data: A NIST-Guided Systematic Review of Technologies, Challenges, and Future Directions. *Information*, *17*(2), 148. https://doi.org/10.3390/info17020148

20. Abuhammad, S. (2025). Strengthening ethical practices of patient data confidentiality and sharing among nurses in the artificial intelligence-driven healthcare era. *Sage Open Nursing*, *11*, 23779608251398113. https://doi.org/10.1177/23779608251398113

21. Shelat, V. G. (2025). Respecting privacy and upholding confidentiality: core ethical duties. *Singapore medical journal*, *66*(12), 685. https://doi.org/10.4103/singaporemedj.SMJ-2025-147

22. Ienca, M., Ferretti, A., Hurst, S., Puhan, M., Lovis, C., & Vayena, E. (2018). Considerations for ethics review of big data health research: A scoping review. *PloS one*, *13*(10), e0204937.

Тип лицензии CC: Attribution 4.0 International (CC BY 4.0)

23. Bibbins-Domingo, K., Brubaker, L., & Curfman, G. (2025). The 2024 revision to the Declaration of Helsinki: modern ethics for medical research. *Jama*, *333*(1), 30-31. https://doi.org/10.1001/jama.2024.22530

Список литературы:

1. Almaghrabi N. S., Bugis B. A. Patient confidentiality of electronic health records: A recent review of the Saudi literature // Dr. Sulaiman Al Habib Medical Journal. 2022. V. 4. №3. P. 126-135. https://doi.org/10.1007/s44229-022-00016-9

2. McNair L. Ethical and regulatory oversight of clinical research: The role of the Institutional Review Board // Experimental Biology and Medicine. 2022. V. 247. №7. P. 561-566. https://doi.org/10.1177/15353702221078216

3. Alharbi M. F. Does electronic health record implementation enhance hospital efficiency and patient outcomes? A comprehensive systematic review // Sage Open. 2025. V. 15. №3. P. 21582440251359791.

4. El Emam, K., Rodgers, S., & Malin, B. (2015). Anonymising and sharing individual patient data. *BMJ*, *350*. https://doi.org/10.1136/bmj.h1139

5. European Parliament and Council. General Data Protection Regulation (GDPR). Regulation (EU) 2016/679. 2016.

6. Fisher Z., Xu T., Jost E., Forlenza G. P., Voida S. 976-P: Data Privacy and Trust Concerns among Adolescent and Young Adults (AYAs) with T1D Using Hybrid-Closed Loop Systems // Diabetes. 2025. V. 74. №Supplement_1. P. 976-P.

7. OECD. Health Data Governance for the Digital Age: Implementing the OECD Recommendation on Health Data Governance, OECD Publishing, Paris, 2022. https://doi.org/10.1787/68b60796-en

8. Heggie V. New perspectives: four unsung heroes of diabetes research // Diabetes Care. 2026. V. 49. №2. P. 216-222.

9. Al Zaabi M., Alhashmi S. M. Big data security and privacy in healthcare: A systematic review and future research directions // Information Development. 2026. V. 42. №2. P. 907-921.

10. Kaye J., Whitley E. A., Lund D., Morrison M., Teare H., Melham K. Dynamic consent: a patient interface for twenty-first century research networks // European journal of human genetics. 2015. V. 23. №2. P. 141-146. https://doi.org/10.1038/ejhg.2014.71

11. Zhu S., Saravanan V., Muthu B. A. Achieving data security and privacy across healthcare applications using cyber security mechanisms // The Electronic Library. 2020. V. 38. №5-6. P. 979-995. https://doi.org/10.1108/EL-07-2020-0219

12. Boadu E. O., Armah G. K. Role-based access control (RBAC) based in hospital management // Int. J. Softw. Eng. Knowl. Eng. 2014. V. 3. P. 53-67.

13. Smith-Mutegi D., Mamo Y., Kim J., Crompton H., McConnell M. Perceptions of STEM education and artificial intelligence: a Twitter (X) sentiment analysis // International Journal of STEM Education. 2025. V. 12. №1. P. 1-18. https://doi.org/10.1186/s40594-025-00527-5

14. Mittelstadt B. D., Floridi L. The ethics of big data: current and foreseeable issues in biomedical contexts // Science and engineering ethics. 2016. V. 22. №2. P. 303-341. https://doi.org/10.1007/s11948-015-9652-2

15. Rehm H. L., Page A. J., Smith L., Adams J. B., Alterovitz G., Babb L. J., Rodarmer K. W. GA4GH: International policies and standards for data sharing across genomic research and healthcare // Cell genomics. 2021. V. 1. №2. https://doi.org/10.1016/j.xgen.2021.100029

16. Price W. N., Cohen I. G. Privacy in the age of medical big data // Nature medicine. 2019. V. 25. №1. P. 37-43. https://doi.org/10.1038/s41591-018-0272-7

Тип лицензии CC: Attribution 4.0 International (CC BY 4.0)

17. Howe III E. G., Elenberg F. Ethical challenges posed by big data // Innovations in clinical neuroscience. 2020. V. 17. №10-12. P. 24.

18. Semyonov-Tal K. Keeping medical information safe and confidential: a qualitative study on perceptions of Israeli physicians // Israel Journal of Health Policy Research. 2024. V. 13. №1. P. 54. https://doi.org/10.1186/s13584-024-00641-9

19. Zhang S., Singh M. M. Privacy and Security in Health Big Data: A NIST-Guided Systematic Review of Technologies, Challenges, and Future Directions // Information. 2026. V. 17. №2. P. 148. https://doi.org/10.3390/info17020148

20. Abuhammad S. Strengthening ethical practices of patient data confidentiality and sharing among nurses in the artificial intelligence-driven healthcare era // Sage Open Nursing. 2025. V. 11. P. 23779608251398113. https://doi.org/10.1177/23779608251398113

21. Shelat V. G. Respecting privacy and upholding confidentiality: core ethical duties // Singapore medical journal. 2025. V. 66. №12. P. 685. https://doi.org/10.4103/singaporemedj.SMJ-2025-147

22. Ienca, M., Ferretti, A., Hurst, S., Puhan, M., Lovis, C., & Vayena, E. Considerations for ethics review of big data health research: A scoping review // PloS one. 2018. V. 13. №10. P. e0204937.

23. Bibbins-Domingo K., Brubaker L., Curfman G. The 2024 revision to the Declaration of Helsinki: modern ethics for medical research // Jama. 2025. V. 333. №1. P. 30-31. https://doi.org/10.1001/jama.2024.22530

Поступила в редакцию
12.09.2026 г.

Принята к публикации
27.09.2026 г.

Ссылка для цитирования:

Valizada Kh., Alizade Ya., Qurbanova G., Guliyeva A., Jafarli Z. Research Ethics and Patient Confidentiality Challenges in Healthcare Management // Бюллетень науки и практики. 2026. Т. 12. №11. С. 592-600. https://doi.org/10.33619/2414-2948/132/67

Cite as (APA):

Valizada, Kh., Alizade, Ya., Qurbanova, G., Guliyeva, A., & Jafarli, Z. (2026). Research Ethics and Patient Confidentiality Challenges in Healthcare Management. *Bulletin of Science and Practice, 12*(11), 592-600. https://doi.org/10.33619/2414-2948/132/67

Тип лицензии CC: Attribution 4.0 International (CC BY 4.0)