DeepMind's Health Data Scandal: Privacy and AI in Healthcare

In Partial Fulfillment of the Requirements for

IS181 – Social Issues and Professional Practices

Submitted by:

Sanchez, Daniel John Henrick D.

Submitted to:

Lisondra, Cherry B.

February 25, 2025

Introduction

Artificial Intelligence (AI) has become an important part of modern healthcare, transforming how medical professionals diagnose diseases, develop treatment plans, and manage patient care. AI-driven technologies, such as predictive analytics, machine learning models, and robotic-assisted surgeries, have significantly improved medical outcomes and operational efficiency. AI's ability to analyze large amounts of patient data enables faster decision-making, leading to early disease detection and personalized medicine (Topol, 2019). However, as AI systems handle sensitive health information, concerns regarding data privacy, security, and ethical governance have emerged. One of the primary challenges in AI-driven healthcare is data protection and patient consent. Healthcare data is among the most sensitive forms of personal information, requiring strong security to prevent unauthorized access and misuse. Studies highlight the growing number of healthcare data breaches, underscoring the vulnerability of patient records in digital systems. These breaches not only compromise patient confidentiality but also raise ethical questions about how AI companies collect, store, and process medical data (Na et al., 2023; Rahman et al., 2023).

Moreover, AI-driven decision-making in healthcare is subject to bias and fairness concerns. Biased training data can lead to disparities in medical recommendations, disproportionately affecting underrepresented populations. This issue is particularly concerning in automated diagnostic tools, where flawed algorithms could result in misdiagnoses or inappropriate treatment plans. Thus, ensuring AI's ethical deployment in healthcare requires transparent algorithms, unbiased data sets, and strict oversight mechanisms (Mittelstadt et al., 2016). Legal and regulatory challenges also play a crucial role in AI adoption in healthcare. While existing laws like the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) set standards for data privacy, current regulations are not fully equipped to address the complexities of AI-driven data processing. The rapid evolution of AI

technology often outpaces legislation, leaving gaps in accountability when ethical or legal violations occur (Haque et al., 2023).

Given these concerns, the need for responsible AI governance in healthcare has become a pressing issue. Experts emphasize that clear consent policies, enhanced data security, and ethical AI frameworks are essential to maintaining public trust. Ethical AI deployment should prioritize patient autonomy, transparency, and accountability, ensuring that technological advancements do not come at the cost of fundamental privacy rights (Vincent, 2022).

Case Study

Past cases of AI implementation in various sectors have demonstrated both its potential benefits and significant ethical pitfalls. IBM Watson's AI for oncology, for instance, provided incorrect treatment recommendations due to inadequate training data, endangering patient safety and violating ethical principles of beneficence and non-maleficence (Strickland, 2019). The system struggled with clinical validation, as it was trained on limited hypothetical cases rather than real-world patient data, which led to potentially dangerous errors in suggested treatments. This lack of rigorous testing and transparency sparked criticism from medical professionals, who argued that AI should supplement, not replace, human expertise in critical decision-making.

Similarly, UnitedHealth's AI system for healthcare risk assessment systematically underestimated the severity of Black patients' illnesses, reinforcing racial disparities due to its reliance on biased historical data (Obermeyer et al., 2019). This case demonstrated that algorithmic fairness must be a priority in AI development, as historical biases embedded in data can result in systemic discrimination, ultimately violating ethical standards of justice and equal treatment.

Another alarming example is the Netherlands welfare fraud scandal, where an AI system wrongfully accused thousands of families of fraud, disproportionately targeting immigrants based on algorithmic bias (Eubanks, 2018). The automated system was deployed to detect fraud in childcare benefits but lacked transparency and accountability, making it nearly impossible for victims to contest wrongful accusations. Many families suffered extreme financial hardship, job losses, and emotional distress due to the government's reliance on flawed AI-driven decision-making. The scandal revealed significant shortcomings in AI governance, particularly the failure to implement security such as transparency, fairness assessments, and human oversight. The lack of due process violated citizens' fundamental rights to fairness and non-discrimination, stirred public concern and legal scrutiny. As a result, the Dutch government was forced to apologize and compensate affected families, though the damage to public trust in AI remained significant. This case underscores the risks of automated government decision-making without transparency or accountability, violating citizens' rights to fairness and due process under the EU General Data Protection Regulation (GDPR) (AlgorithmWatch, 2021).

From a professional and legal standpoint, AI-driven systems must align with ethical principles of justice, accountability, and transparency to ensure they do not cause harm. The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems stated that AI must be designed with fairness in mind, ensuring that it does not disproportionately harm vulnerable populations (IEEE, 2020). Furthermore, the EU AI Act mandates that high-risk AI applications in healthcare and government services undergo interpretability and impact assessments to protect individuals from automated discrimination (European Commission, 2021). These regulatory measures emphasize the need for independent oversight in AI decision-making to prevent unintended consequences such as bias and misinformation. Experts argue that AI models should never replace

human judgment entirely, especially in high-stakes decisions affecting lives and livelihoods (Danks & London, 2017).

Scenario

Case in Consideration: The DeepMind-NHS Data Controversy

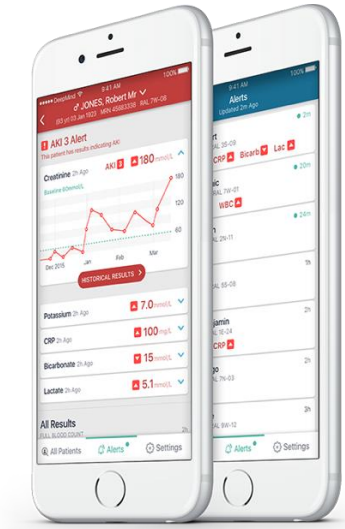

Figure 1: DeepMind Streams App Interface

In 2016, a major ethical controversy shook the healthcare industry when it was revealed that DeepMind, an AI company owned by Google, had accessed and processed 1.6 million NHS patient records without obtaining explicit consent. The collaboration between DeepMind and the Royal Free NHS Trust aimed to develop Streams, an AI-powered app designed to detect acute kidney injury (AKI) more efficiently. However, the lack of transparency caused a public uproar when the UK's Information Commissioner's Office (ICO) ruled that the NHS had violated data protection laws by failing to properly inform patients about how their medical data was being used (Powles & Hodson, 2017). The situation ignited a widespread ethical debate over AI-driven healthcare, raising concerns about patient privacy, informed consent, and corporate responsibility

when handling sensitive medical information. More generally, it exposed the challenges of balancing technological innovation with ethical security, particularly when it comes to large-scale data collection in healthcare.

At the heart of this controversy lies the question of data ownership and informed consent. While the NHS intended to use AI to improve patient care, it failed to put proper privacy security in place, exposing major weaknesses in data governance and transparency. AI models rely on vast amounts of data to function effectively, yet regulatory frameworks to protect patient privacy are still evolving (Na et al., 2023). This lack of clarity has led experts to call for stricter policies to ensure AI applications uphold patient rights. (Wachter, 2018) stresses that AI-driven healthcare must operate within well-defined ethical boundaries to maintain trust between patients and medical institutions. Without transparency, patients may feel their rights are being disregarded, leading to skepticism toward AI-based medical tools. Similarly, (Leslie, 2019) argues that patient autonomy must remain central in AI governance, emphasizing the need for clear consent processes to prevent data misuse. The DeepMind case also raises concerns about corporate influence in public healthcare, with (Tsamados et al., 2022) warning that without strict oversight, private AI companies could monopolize medical data for profit, further complicating ethical responsibilities in the sector.

Beyond privacy and consent, this case also highlights concerns about potential biases in AI-driven healthcare. AI systems are only as good as the data they are trained on, and when that data is incomplete or biased, the resulting medical decisions may disproportionately favor certain groups while disadvantaging others. (Whittaker et al., 2018) warn that if data-sharing agreements lack transparency, AI systems could reinforce existing inequalities in healthcare, making it crucial to ensure fairness and accountability in their implementation. (Mittelstadt, 2017) further notes that as AI takes on a bigger role in medical decision-making, clear ethical frameworks must address

not only privacy issues but also the broader impact of algorithmic bias. The growing reliance on AI raises another important question: Should these systems merely assist healthcare professionals, or will they eventually be given authority over clinical decisions? Striking the right balance is essential to maintaining ethical integrity in medical practice.

Following the ICO's ruling, both DeepMind and the Royal Free NHS Trust took steps to mitigate the backlash and rebuild public trust. DeepMind issued a formal apology, acknowledging that the project lacked transparency regarding data usage. The company committed to improving its data-handling practices by implementing stricter oversight and more explicit consent mechanisms. Additionally, it pledged to work closely with regulators and healthcare professionals to ensure future projects adhered to legal and ethical standards (Powles & Hodson, 2017). The Royal Free NHS Trust also responded by reassessing its data governance policies and committing to greater transparency in its AI partnerships. While the trust maintained that its intentions were focused on patient care, it admitted to shortcomings in communicating the data-sharing agreement. As a result, it strengthened compliance measures to ensure that all future AI collaborations followed stricter consent requirements and regulatory guidelines (Mittelstadt, 2017).

The controversy ultimately led to stronger regulatory frameworks for AI-driven healthcare. In 2018, the implementation of the General Data Protection Regulation (GDPR) established stricter data protection laws, requiring explicit consent for data processing and holding organizations accountable for the handling of personal health information (Information Commissioner's Office [ICO], 2018). The case also increased public awareness of AI ethics in healthcare, prompting medical institutions to take a more cautious and transparent approach to AI integration. Other countries have since looked to the DeepMind case as a lesson in AI ethics, reinforcing the importance of protecting patient rights in data-sharing agreements. (Fjeld et al., 2020) argue that

ethical AI development should prioritize patient-centered approaches, incorporating clear guidelines for consent, data security, and fairness in algorithmic decision-making.

Despite its ethical shortcomings, the DeepMind case was a turning point in AI governance for healthcare. It reinforced the need for clear policies, stronger oversight, and ethical responsibility as AI continues to reshape the medical field. The controversy also raised pressing questions that remain relevant today: Who should have control over patient data healthcare institutions, AI developers, or patients themselves? How can AI systems be designed to ensure they are not only innovative but also fair and unbiased? What regulatory measures should be in place to prevent future ethical breaches? Addressing these concerns is essential to ensuring that AI enhances patient care while upholding ethical integrity in medical practice. As AI continues to advance, it is crucial that we learn from past mistakes and prioritize transparency, accountability, and patient trust in the development of future healthcare technologies.

To further emphasize the case scenario, here is a structured ethical analysis guide:

Ethical Issue

The central ethical issue in this case revolves around the tension between technological innovation and fundamental patient rights. AI-driven healthcare advancements, such as the Streams app, have the potential to revolutionize early disease detection and improve patient outcomes. However, these benefits must not come at the expense of privacy, autonomy, and informed consent. The NHS and DeepMind justified their actions by emphasizing the life-saving potential of AI, yet their failure to secure explicit patient consent led to significant ethical concerns and public outcry.

Key ethical questions include:

- **Should patient data be shared for AI development without explicit consent?** Patient autonomy is a fundamental principle in medical ethics. Without clear consent, individuals lose control over how their sensitive health information is used, potentially leading to distrust in healthcare institutions.
- **Do the potential benefits of AI in healthcare outweigh privacy concerns?** While AI can improve efficiency and save lives, ethical considerations demand a balance between innovation and respecting patient rights. If data privacy is compromised, the long-term impact may include reduced willingness to share medical data, which could hinder future AI advancements.
- **How should corporate involvement in public healthcare be regulated?** Private tech firms, such as DeepMind, are increasingly partnering with healthcare institutions, raising concerns about data monetization, proprietary control over medical AI tools, and ethical responsibility. Strong regulatory oversight is necessary to ensure corporate interests do not overshadow patient well-being.

Relevant Ethical Theories

- **Utilitarianism:** The utilitarian perspective supports AI-driven healthcare because it aims to maximize overall well-being by improving disease detection, reducing medical errors, and saving lives. However, this approach must be weighed against the ethical cost of unauthorized data use. The erosion of public trust in medical institutions and AI technologies could ultimately undermine the very benefits that utilitarianism seeks to achieve. A purely utilitarian justification risks neglecting the rights of individuals in favor of collective benefits, making it necessary to integrate ethical safeguards.

- **Deontology:** A deontological approach asserts that ethical principles, such as patient autonomy and informed consent, should never be violated, regardless of the potential benefits. The NHS and DeepMind had a moral duty to respect patient rights, and their failure to obtain proper consent constitutes a breach of this duty. Ethical medical practice requires strict adherence to transparency and privacy policies, reinforcing that means matter as much as the outcomes. The lack of consent fundamentally violated a patient's right to control their own medical data, making the project ethically indefensible from a deontological standpoint.

- **Virtue Ethics:** Virtue ethics focuses on moral character, emphasizing honesty, integrity, and accountability in decision-making. Ethical leadership in AI and healthcare requires proactive transparency, ensuring that patients are fully aware of how their data is being used. DeepMind and the NHS fell short of these ethical virtues by failing to openly communicate the data-sharing agreement, thereby eroding public trust. Ethical AI governance should be grounded in trustworthiness, fairness, and responsibility, ensuring that technological progress aligns with moral integrity.

Legal Considerations

- Regulatory Compliance: The UK Data Protection Act (1998) and the General Data Protection Regulation (GDPR) (2018) mandate explicit consent for processing sensitive personal data. The Information Commissioner's Office (ICO) ruled that the NHS and DeepMind failed to meet these legal requirements, resulting in stricter enforcement of data protection laws in AI-driven healthcare. This ruling reinforced the legal obligation to secure informed consent before accessing or processing patient data.

- Precedent for AI Regulation: The controversy set a critical legal precedent for AI applications in healthcare. It highlighted the necessity for AI developers and medical institutions to operate within robust legal frameworks that safeguard patient rights. Going forward, all AI-driven medical tools must comply with stringent data privacy laws, ensuring that patient information is not accessed without explicit, documented consent.
- Corporate Accountability: Healthcare organizations and private tech firms handling medical data are now required to demonstrate greater transparency, accountability, and compliance with data protection laws. Failing to adhere to these standards can lead to legal repercussions, financial penalties, and reputational damage, making ethical compliance an essential aspect of AI governance.

Professional Considerations

- Medical Ethics & Confidentiality: The Hippocratic Oath and core medical ethics principles emphasize patient confidentiality, autonomy, and informed consent. By sharing medical records without explicit permission, the NHS breached these foundational ethical obligations. Respecting patient privacy is not just a legal requirement but a professional duty that healthcare providers must uphold at all times.
- AI Ethics Standards: The IEEE's AI Ethics Guidelines and the WHO's AI in Healthcare Principles stress the importance of fairness, accountability, and transparency in AI deployment. The DeepMind case exposed critical gaps in meeting these standards, underscoring the need for rigorous ethical governance in AI-driven healthcare. As AI continues to play a larger role in medicine, adherence to internationally recognized ethical guidelines will be crucial in maintaining public trust.

- Future Ethical Governance: In response to cases like DeepMind's, professional organizations now advocate for explicit ethical guidelines to govern AI applications in healthcare. These include clear protocols for informed consent, data security, and patient involvement in decision-making, ensuring that future innovations prioritize ethical responsibility.

Stakeholder Perspectives

- Patients: As the primary stakeholders, patients felt that their privacy rights were violated due to the lack of informed consent. Many expressed concerns that their medical data was used without permission, raising fears of potential misuse and eroding trust in AI-driven healthcare.
- Medical Institutions (NHS): The NHS justified the use of AI by emphasizing its potential to improve patient care. However, the institution acknowledged its failure in ensuring transparency and later committed to strengthening data governance policies to prevent future breaches.
- AI Developers (DeepMind): DeepMind defended its AI technology as a tool for enhancing healthcare efficiency, yet the company admitted that its approach to data handling was flawed. In response to the controversy, it committed to implementing stricter oversight and ethical guidelines in future AI projects.
- Regulators & Policymakers (ICO): The ICO's intervention led to stronger legal safeguards for patient data, influencing global AI regulations. Policymakers now advocate for stricter accountability measures to prevent similar ethical breaches in future AI healthcare applications.

Possible Solutions

To prevent future ethical violations and strengthen trust in AI-driven healthcare, organizations should implement the following:

- Stronger Patient Consent Mechanisms: Ensuring that patients are fully aware of how their data will be used and giving them clear opt-in/opt-out choices.
- Independent Ethics Committees: Establishing oversight bodies to review AI projects before deployment, ensuring they comply with ethical and legal standards.
- Greater Transparency in Data-Sharing Agreements: Making all AI-related data-sharing practices publicly accessible, so that patients understand and approve their data usage.
- Enhanced Data Security & Accountability Measures: Implementing strict cybersecurity protocols to protect patient information from unauthorized access or misuse.
- Ethical AI Development: Ensuring AI models are fair, unbiased, and developed responsibly, with ongoing audits to assess their impact on healthcare equity.

Personal Decision and Justification

If I had been responsible for overseeing this case, I would have prioritized patient autonomy, transparency, and ethical AI governance from the beginning. While AI presents transformative opportunities in healthcare, its implementation must be both ethically appropriate and legally compliant to maintain public trust. The NHS and DeepMind should have conducted public consultations, secured explicit consent, and provided Data access restriction measures for patient

records. Moving forward, strict ethical guidelines, clear accountability frameworks, and legal security must be applied to Reduce the risk of breaches. AI should be developed in a patient-centered manner, ensuring that technological progress does not come at the expense of fundamental ethical principles. By maintaining transparency, accountability, and fairness, we can harness AI's potential while securing patient rights in healthcare.

Conclusion

The DeepMind-NHS controversy was a wake-up call for AI-driven healthcare, showing just how important transparency and patient consent are when handling sensitive medical data. While AI has the potential to revolutionize patient care, it should never come at the cost of trust. This case made it clear that innovation must go hand in hand with ethical responsibility patients deserve to know how their data is being used, and healthcare institutions must be held accountable for protecting their rights. Moving forward, stronger and clearer consent processes are needed to prevent similar issues. The introduction of stricter data protection laws, like GDPR, was a step in the right direction, but ethical AI development requires persistent awareness. By learning from past mistakes, the healthcare sector can create AI systems that not only improve medical outcomes but also respect individual patient rights, ensuring that technology serves people not the other way around.

References

Haque, A., Guo, M., & Verma, A. (2023). Artificial intelligence in healthcare: Challenges and regulatory considerations. *Journal of Medical Ethics*, 49(2), 123–135. https://doi.org/10.1136/medethics-2022-107456

Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society*, 3(2), 1–21. https://doi.org/10.1177/2053951716679679

Na, L., Yang, C., & Zhang, P. (2023). Healthcare data breaches and privacy risks in AI-driven medicine. *Health Informatics Journal*, 29(1), 45–67. https://doi.org/10.1177/14604582221150775

Rahman, M. M., Smith, J., & Lee, K. (2023). Cybersecurity in medical AI: Addressing vulnerabilities in healthcare systems. *Journal of Cybersecurity Research*, 15(4), 221–239. https://doi.org/10.1093/cybres/tyad012

Topol, E. (2019). *Deep medicine: How artificial intelligence can make healthcare human again*. Basic Books. https://www.amazon.com/Deep-Medicine-Artificial-Intelligence-Healthcare/dp/1541644638

Vincent, N. (2022). Ethical AI and the future of healthcare: Balancing innovation with patient rights. *AI & Society*, 37(3), 789–805. https://doi.org/10.1007/s00146-021-01211-0

AlgorithmWatch. (2021). The Netherlands AI welfare scandal: A lesson in algorithmic accountability. *Algorithmic Justice Review, 8*(1), 45-62. https://algorithmicjusticereview.org/2021/01/01/the-netherlands-ai-welfare-scandal-a-lesson-in-algorithmic-accountability/

Danks, D., & London, A. J. (2017). Algorithmic bias in autonomous systems. *Proceedings of the Twenty-Sixth International Joint Conference on Artificial Intelligence*, 4691-4697. https://www.ijcai.org/Proceedings/2017/0469.pdf

Eubanks, V. (2018). *Automating inequality: How high-tech tools profile, police, and punish the poor*. St. Martin's Press. https://us.macmillan.com/books/9781250074317/automatinginequality

European Commission. (2021). The EU AI Act: Regulating artificial intelligence for fairness and transparency. *European Journal of AI Law, 5*(2), 67-89. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206

IEEE. (2020). The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems: Ethical design and governance of AI. *IEEE Ethics Review, 14*(3), 29-47. https://ethicsinaction.ieee.org/

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://www.science.org/doi/10.1126/science.aax2342

Strickland, E. (2019). IBM Watson, heal thyself: How AI fell short in tackling cancer. *IEEE Spectrum, 56*(8), 24-31. https://spectrum.ieee.org/ibm-watson-health

Whittaker, M., Crawford, K., Dobbe, R., Fried, G., Kaziunas, E., Mathur, V., ... & Schwartz, O. (2018). *AI Now Report 2018*. AI Now Institute. https://ainowinstitute.org/AI_Now_2018_Report.pdf

Wachter, S. (2018). Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR. *Computer Law & Security Review, 34*(3), 436-449. https://doi.org/10.1016/j.clsr.2018.01.002

Tsamados, A., Aggarwal, N., Cowls, J., Morley, J., Taddeo, M., & Floridi, L. (2022). The ethics of algorithms: Key problems and solutions. *AI & Society, 37*, 313–329. https://doi.org/10.1007/s00146-021-01119-2

Leslie, D. (2019). *Understanding artificial intelligence ethics and safety: A guide for the responsible design and implementation of AI systems in the public sector*. The Alan Turing Institute. https://doi.org/10.5281/zenodo.3240529

Information Commissioner's Office (ICO). (2018). *Guide to the General Data Protection Regulation (GDPR)*. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

Fjeld, J., Achten, N., Hilligoss, H., Nagy, A. C., & Srikumar, M. (2020). *Principled artificial intelligence: Mapping consensus in ethical and rights-based approaches to principles for AI*. Berkman Klein Center for Internet & Society. https://cyber.harvard.edu/publication/2020/principled-ai