Ethical Issues in Sharing Health Data

I. PERSONAL REFLECTION ON OPEN DATA

A. Definition and Key Insights on Open Data

Open data refers to data that is made freely available to everyone, with no restriction on access, use or redistribution, in the interest of transparency, innovation, and public engagement [4]. It was really interesting to see how each of the lectures and seminars looked at different definitions and takes on open data. Janssen et al. [2] insisted that open data involves more than just publishing data; it means providing the public the opportunity to review, analyze, and work with data for a variety of purposes. He coined the idea of "people power," which I found compelling because it connects open data to larger policy and social goals such as better public policy and service delivery.

One of the strong messages from our deliberations was that open data has considerable potential to fuel innovation in sectors such as health, education, and the environment. Researchers and developers are granted the ability to explore new avenues to complex problems in an open data environment. Open health data can improve public health strategies by providing better access to information on health trends. For example, World Bank [6] suggests that this will improve public health, as well as awareness among the general population.

There were also discussions about open data challenges and ethical issues. While the implementation of open data is a good concept to provide citizens with more power, it poses risks when there are personal data [3]. Given the ballooning of data and the sophistication of data analytics tools, the new question to consider is whether the effectiveness of anonymization techniques (previously considered as one solution to the privacy problem) to reduce the risk of re-identification. Here lies an ethical dilemma: balancing the transparency that is essential for removing power dynamics with the preservation of the right to privacy.

How open should open-data be; open-data is a copious initiative and one of the strong ethical dillemmas on the open-data side. Data access can enhance governance and services but it also undermines people's privacy. This double-edged sword can best be seen in fields such as healthcare, where sensitive data should be treated carefully to be avoided.

B. Reflections on How These Discussions Have Influenced My Thinking

Before the lectures and discussions, I had primarily seen open data as a means of democratizing access to information. I thought: surely, once data is open, society will become more informed and engaged. Concepts such as open data as a public good, where information should be free from copyright restrictions and openly available to generate public benefit [5], were ideas that really resonated with me back then.

With further reflection, after listening to the conversations, I realize that open data is actually a much more ethically and philosophically complicated question than I was aware of at the outset. While open data may hold the key to innovation and social evolution, it also poses fundamental questions of privacy and security. In the healthcare domain, for example, the sensitive nature of such data means that open data poses significant risks whenever private information originates from the open world. That balancing act of transparency with privacy isn't as simple as I had imagined.

Indeed, I was mulling over how open data could celebrate transparency in government and public services. Open data allows citizens to track public policies and check governments, a fundamental element of any democracy. Open data democratizes the governance process and makes it practical for citizens to participate and have access to information. But I have learned that openness cannot supersede privacy and the rights of individuals.

These conversations made me think about the digital divide, in that there are groups or individuals that have limited (or no) access to (or relevant know- how to use) open data. It will exacerbate existing inequalities, as some parts of the population are disadvantaged in participating in the digital age. The reality of open data is that inclusive open data initiatives are what we need, not open data for the technically talented.

Lastly, the more nuanced conversations around open data made me think twice about the position I occupy in the data- driven world. Being a person who deals with data, I now understand how important ethical data practices are, especially in balancing privacy and transparency. Moving forward, I will be much more conscious of the ethical considerations of the information I am working with and strive to ensure that I do not contribute to any form of data-centric harm.

So far from these discussions I have learnt a lot about open data and its potential benefits, as well as ethical concerns around it. Today, I view open data as a phenomenal tool for accelerating social progress but one that needs to be handled delicately so that we can keep the scales balanced between transparency and the rights of the individual.

II. ETHICAL ANALYSIS OF THE CASE STUDY

A. Case Study: Sharing of Health Data for Medical Research

This case study focuses on a healthcare organization that has decided to share patient health data with a research facility. This partnership aims to accelerate research into common illnesses by analyzing patient records to reach conclusions with novelty, which can improve treatment and the delivery of care. Sensitive patient information metrics such as demographics, diagnoses, treatments, and results from medical tests are included in the data that the cybercriminals are sharing. However, this poses major ethical dilemmas related to privacy, consent, and the appropriate utilization of patient information.

The hospital is a public healthcare organization, and the institution is a nonprofit research organization focusing on medical technology. Anonymization is meant to render data-unidentifiable to a level that it can be safely shared, but given that the data has patient information that could be sensitive, the question, on how safe it is, remains, since one of the hospitals data even had non-anonymized unidentifiable information included. Many patients also questioned whether they had adequately consented to having their data used in this research and whether their privacy would be assured.

The hospital has an agreement with the research institution to share data with multiple safeguards to protect patients' privacy, but patients are still worried about data breaches, deanonymization or the security of sensitive health information.

B. Explanation of the Case Study

This case involves a healthcare organization that is a pub- licly funded hospital that collects information on its patients' health in detail. This data can cover a broad spectrum of medical information, from basic demographic information (age, sex, address) to comprehensive health records (diagnoses, treatments, lab results). That data is a goldmine for medical researchers, and the hospital has agreed to share it with a nonprofit research organization working to develop new chronic disease treatments.

The research institute aims to use the data to identify patterns related to chronic diseases and develop better therapies. The organization has said the data will be used to discover breakthroughs that could not only benefit current patients but future generations by advancing medical knowledge.

However, the data-sharing agreement covers non- anonymized as well as anonymized data. Although anonymization protects patient identity, the process must remain effective.

There is a risk for a medical provider to be able to de-anonymize the anonymized patient data and trace it back to individual patients. In addition, multiple patients claim that they were not fully informed about the data-sharing agreement and that they did not give explicit permission for their data to be shared in this way.

Beyond privacy concerns, questions have emerged about the fairness of the research process. Are all patients treated the same when it comes to their data being shared, and do they all have equal access to the benefits that come from the research? Particularly from the principlist position that highlights justice, non-maleficence, beneficence, and autonomy as central rules of thumb in healthcare ethics, these issues are particularly important.

C. Ethical Frameworks Applied

In this section, we will use deontological ethics and prin- ciplism to examine the ethical questions implicated with the sharing of health data. This means that these two frameworks offer different angles on making sense of privacy, consent, and the potential benefits of research for the society.

Deontological ethics emerged from the work of Immanuel Kant [7]; it emphasizes the ethical nature of an action inde- pendent of its consequences. As the approach states, people have rights, duties and responsibilities and it is those that need to point in whichever direction is followed – regardless of possible good or bad consequences that may follow. So, one ethical concern to take away from this perspective relates to the surface level concern that data will infringe on others autonomy or privacy.

In this particular case scenario, deontological ethics focuses on the importance of the healthcare organization to fulfill its obligations and duties to honor the rights of its patients. Under this framework, we must respect the fact that the patients have a right to privacy and control over their personal data and any breach of this would be deemed as ethically incorrect, intentional or otherwise. Kantian ethical theory maintains that the moral precept to treat human beings as ends in themselves, and never merely as means to an end, is a fundamental moral principle [7]. There would therefore be a violation of patients' autonomy and dignity where their personal data are used for research purposes without their clear and explicit consent.

On the other hand, deontological ethics advocates that individuals have the right to know how their data will be controlled. That suggests that if patients were not aware of the extent of the data-sharing agreement, then the ethical burden of responsibility weighs on the hospital and the research organization. The absence of clear image in terms of points of sales and therefore not revealing the total now a days sales goes against one amongst the fundamental principle within the medical ethics that is "informed consent"

Kant [7] would argue that in spite of what benefits the research may bring to society, the patients' rights to control their data should not be sacrificed for the greater good. This is an example of a central ethical dilemma in health care and data research: Is the possible benefit of medical research enough to outweigh the potential compromise of patient privacy and autonomy? The answer is no, because doing so would vio- late the inviolable moral rights of individuals, according to deontological ethics.

The autonomy questions are particularly acute for health data. Patient autonomy is at the center of the practice of informed consent, which requires that patients be informed of and consent to how their data will be used. By Kantian standards, what this means is they need to do due diligence to communicate to patients how their data will be shared and for what ends. In the absence of the clarity in treatment options provided by patients, the hospital and research institution would be exercising improper patient autonomy in order to further medical research.

The approach of principlism, originally articulated by Beauchamp and Childress [8], is considerably more flexible. This framework consists of four principles where autonomy, beneficence, non-maleficence, and justice are directly related. However, each of these principles informs us in its own way on how to determine whether sharing your health data will inherently make you an aggressor of someone's rights.

Principle of Autonomy provides that individuals have control over their own lives and bodies and should have control over their personal data as well. Autonomy is at the core of this case, because patients should decide how their personal health data is utilized. Following the philosophy of principlism, patients need to be fully aware of the ways in which their data could potentially be used, and they need to explicitly consent to have it shared with a third party. This ensures that they are treated as independent agents with the right to make decisions pertaining to their privacy [8]. If the patients gave no informed consent, or did not understand the implications of data-sharing agreement, the ethical responsibility lies with the hospital and the research institution.

Autonomy (people's right to make choices) is one of the principles that supports the ethical framework because it also protects individual rights over personal information. Patients must know precisely what will be done with their data, and patients should provide consent only when they have had their data fully explained. Autonomy in this context is not alternative options; it is informed alternative options — options where patients understand what data sharing means for themselves and others in society more broadly.

The principle of beneficence requires taking action to pro- mote the well-being of others. And in this case, the research in- volves patient data that is expected to advance the science and thus help future generations achieve better health outcomes. Not only current patients but also the general public stands to gain from the development of new treatments for chronic diseases. Thus, beneficence lends support to the data-sharing arrangement at least to some degree, as it may yield significant social benefits [8]. In fact, this principle also stipulates that the value of the research must be considered in the balance with the risk of harm to the patients' privacy.

Although beneficence is an underpinning of the concept of using patient data to improve research, it is not without limitations. It is imperative that the principle balances it out with the least possible harm to patient privacy and trust. These policies are particularly important for research involving human subjects as the potential benefits of the research can often be countered by the possible consequences of breaching patient confidentiality and trust in the healthcare system if the research institution fails to adequately protect patient data and its anonymity. The principle of beneficence would thus require the health care organization to implement the strongest possible safeguards to reduce these risks.

The moral substring of non-maleficence states, do no harm. This is the concern of non-maleficence; if harm impacts the patient such as a violation of their privacy. Concerns about potential de-anonymization or data breaches are also among the main risks, in which patients' personal medical information may be revealed or improperly used [8]. Non-maleficence obligates the hospital and research institution to protect patients' privacy and to ensure that any data which is used in research is appropriately anonymized.

According to the principle of non-maleficence, biases can be avoided by patient data privacy safeguards. Even aggregated datasets are vulnerable to being re-identified if not strong enough anonymization techniques are applied. To mitigate these risks, the hospital and research institution must implement best practices and cutting-edge technologies that ensure data confidentiality and security. Patients should, moreover, be informed of the safeguards for their privacy that have been instituted, so that they can give informed consent to their participation in the data-sharing agreement.

The principle of justice is shown in the equitable distribution of costs and benefits. In terms of health data sharing, justice demands equitable use of patient data and equitable distribution of the benefits of research. Patients deserve to be treated the same, and all patients must have the same access to information about how their data will be used. Furthermore, this principle seeks to make certain that the benefits of the research are not limited to one group and the risks disproportionately borne by another [8]. Thus, any failure to adequately inform all patients or any inequities in the data- sharing process would constitute an ethical violation according to the principle of justice.

Justice extends to the sharing of benefits of the research with patients. If the research leads to new treatments or innovations, it should benefit people with the conditions in question. It is not only the logical and the right thing to do — but justice requires sharing the benefits of the research, not just to the researchers or a few selected individuals, but the wider population of patients who provided their data and would be affected by the new research.

D. Critical Reflection on the Analysis

The deontological approach to this case emphasizes the duty of care and the importance of respecting patients' rights by ensuring that data is used in a manner that patients understand and consent to. This approach may appear inflexible especially in circumstances where the societal benefits of the research are immense. Kantian ethics emphasises the inherent rights of individuals and requires us to treat people as ends in themselves but does not offer much in terms of how we should prioritise these rights against the potential benefits which may arise from medical research.

In instructions, the four principles of autonomy, beneficence, non-maleficence, and justice are a more comprehensive frame- work for addressing data sharing's ethical complexities. Where deontological ethics may leave considerations about patient rights, principlism allows the balance of a broader vision that combines both individual rights and what is good for society- places as hat. For example, principlism suffers from a potential constraint that it may cause conflicts between principles. When social good is being made an issue, beneficence, which values the picture as a whole above anything else for just this single patient, and non-maleficence (minimizing harm to individuals) and these two principles are hard to balanceventertainty.

E. Conclusion

Deep and complicated though they are, the ethical challenges facing medical research involving patient health data cannot escape the keen eye of mankind. Both deontological ethics and principlism spit out fat commissions about the problematic aspects of these challenges. Deontological ethics concerns the intrinsic moral rights of patients, such as both their right to privacy and control over their personal data; principlism meanwhile provides a more flexible approach that reconciles individual rights with public interests. By combining these two approaches, the ethical issues in this case are tackled in a fuller way.

REFERENCES

[1] T. Davies, *The state of open data: Histories and horizons*. Cape Town: African Minds, 2021.

[2] M. Janssen, Y. Charalabidis, and A. Zuiderwijk, "Benefits, adoption barriers, and myths of open data and open government," *Information Systems Management*, vol. 29, no. 4, pp. 258–268, 2012.

[3] R.Kitchin,*Thedatarevolution:Bigdata,opendata,datainfrastructures and their consequences*. London: SAGE Publications, 2014.

[4] Open Data Handbook, "What is open data?," 2021. [Online]. Available: https://opendatahandbook.org.

[5] OpenDataInstitute,*Opendataanditsbenefits*,2022.[Online].Available: https://theodi.org.

[6] World Bank, *Open data for economic growth*, 2020. [Online]. Available: https://data.worldbank.org.

[7] I. Kant, *Groundwork of the Metaphysics of Morals*, 1785. [Online]. Available:https://plato.stanford.edu/archives/win2008/entries/ ethics- deontological.

[8] T. L. Beauchamp and J. F. Childress, *Principles of Biomedical Ethics*, 8th ed. New York: Oxford University Press, 2019.

[9] B. Williams, "Deontological Ethics in Healthcare: The Duty of Informed Consent," *Journal of Medical Ethics*, vol. 46, no. 5, pp. 330–337, 2020. [Online]. Available: https://journalofmedicalethics.bmj.com/content/early/ 2020/01/15/medethics- 2019- 105711.

[10] Johns Hopkins University, *Data Privacy in Healthcare: Ethical Chal- lenges and Solutions*, 2021. [Online]. Available: https://www.jhu.edu.