Anonymization of Data in Healthcare Sector

A policy study

Akshay Bajpai (193079002)
Soham Naha (193079003)
R V Satwik (193079009)
Mohit Agarwala (19307R004)

Outline

- AI in Healthcare
- Anonymization Techniques
- Gaps in existing policies
- Attacks on Anonymization
- Health Dataset and code
- Results and Observations
- References

AI in Healthcare

- Mining health data may lead to faster medical choices, better treatment quality, illness prevention, lower costs, and more creative healthcare solutions.
- Health data is highly sensitive and subject to regulations such as the General Data Protection Regulation (GDPR), which aims to ensure patient’s privacy.
- Anonymization of patient identifiable information is the first and most crucial step in adhering to the requirements and incorporating privacy concerns.

Common Literary Ethical Themes of AI in Healthcare

The dearth of literature on the ethics of AI within low and middle income countries (LMICs), as well as in public health, points to a critical need for further research into the ethical implications of AI within both global and public health

Privacy and security

a. There is a potential for information collected by and for AI systems to be **hacked**. A diagnostic laboratory database in Mumbai was hacked in 2016, during which 35,000 patient medical records were leaked, **inclusive of patient HIV status**.
b. **Proprietary** software : less subject to scrutiny

Common Literary Ethical Themes of AI in Healthcare

Trust in AI applications:

a. Data sharing partnership between Google DeepMind, an AI research company, and the Royal Free London NHS Foundation Trust. Identifiable data from 1.6 million patients was shared with DeepMind with the stated intention of improving the management of acute kidney injuries with a clinical alert app.

b. Whether the quantity and content of the data shared was proportionate to what was necessary to test the app?

c. Why it was necessary for DeepMind to retain the data **indefinitely**?

Common Literary Ethical Themes of AI in Healthcare

Accountability and responsibility for use of AI technology:

a. Harmed by a robotic care provider. Is the burden of responsibility for such harm on the robot manufacturer who wrote the learning algorithm?
b. Autonomous vehicles accidents : The liability of the driver in the case of an accident would be based on his failure to pay attention and intervene?

Common Literary Ethical Themes of AI in Healthcare

Adverse consequences of bias:

a. Bias was yet another transcending ethical theme within the literature, notably the potential **bias embedded within algorithms**.

b. The prevailing concern with algorithms was that they are developed by humans, who are by nature fallible, and **subverted by their own values and implicit biases**

Gaps in the literature

Healthcare was the predominant focus in the ethics literature on AI applications in health, with the **ethics of AI in public health largely absent** from the literature

Overarching ethical concerns about privacy, trust, accountability, and bias, each of which are both **interdependent and mutually reinforcing**

The security of confidential patient data is critical for eliciting patient trust in the use of AI technology for health

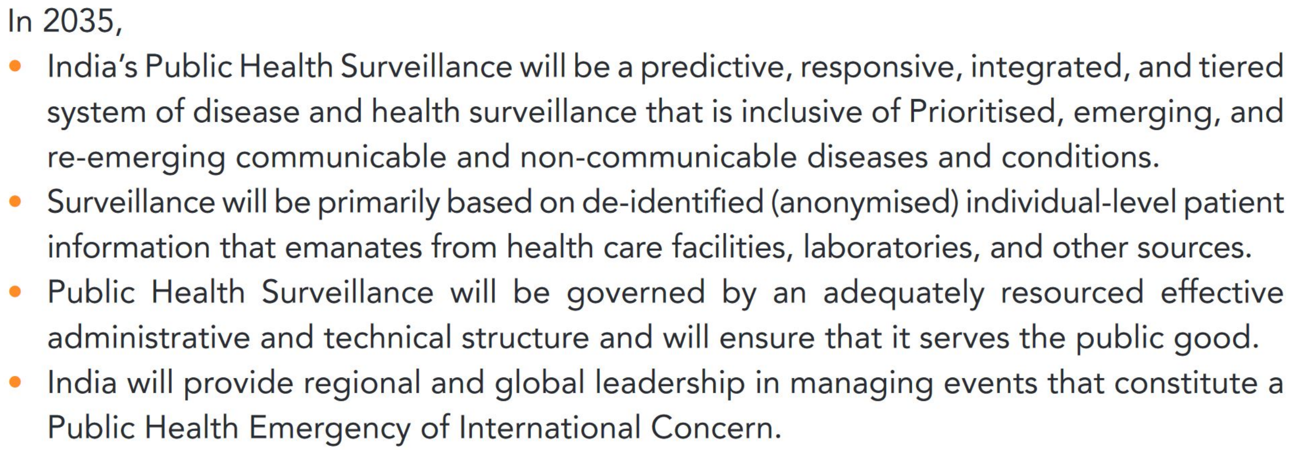
Gaps in the literature

An asymmetry in the literature was the predominant focus on the ethics of AI in healthcare, with less attention granted to public health, including its core functions of health promotion, disease prevention, public health surveillance, and health system planning from a population health perspective.

A second asymmetry in the literature was the focus on high income countries (HICs), and a notable gap in discourse at the intersection of ethics, AI, and health within low and medium income (LMICs). Some articles mentioned the challenges of implementing the technology in low-resource settings.

Gaps in the literature

Surprisingly, the only a **single mention** of data anonymization was provided in the Vision 2035 Public Health Surveillance in India (a White paper) by NITI AYOG

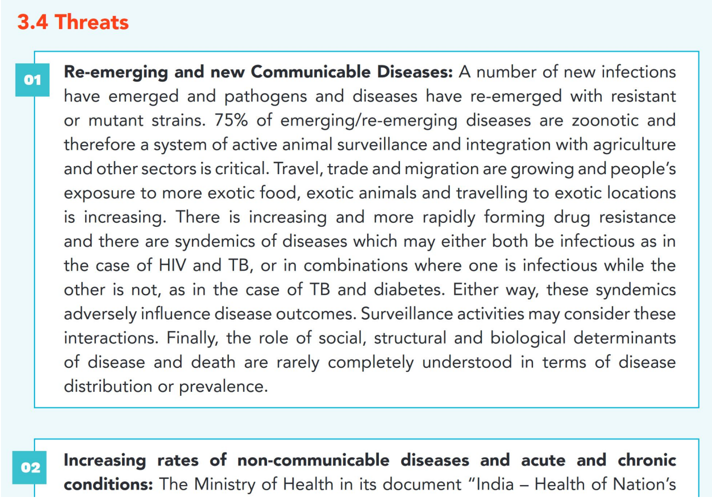


In 2035,

- India's Public Health Surveillance will be a predictive, responsive, integrated, and tiered system of disease and health surveillance that is inclusive of Prioritised, emerging, and re-emerging communicable and non-communicable diseases and conditions.
- Surveillance will be primarily based on de-identified (anonymised) individual-level patient information that emanates from health care facilities, laboratories, and other sources.
- Public Health Surveillance will be governed by an adequately resourced effective administrative and technical structure and will ensure that it serves the public good.
- India will provide regional and global leadership in managing events that constitute a Public Health Emergency of International Concern.

Gaps in the literature

Further in the previous document, the security of the personal data of a patient and deanonymization of the data were not considered as a threat and no metrics / regulations were proposed to safeguard the personal data of a patient



3.4 Threats

01 **Re-emerging and new Communicable Diseases:** A number of new infections have emerged and pathogens and diseases have re-emerged with resistant or mutant strains. 75% of emerging/re-emerging diseases are zoonotic and therefore a system of active animal surveillance and integration with agriculture and other sectors is critical. Travel, trade and migration are growing and people's exposure to more exotic food, exotic animals and travelling to exotic locations is increasing. There is increasing and more rapidly forming drug resistance and there are syndemics of diseases which may either both be infectious as in the case of HIV and TB, or in combinations where one is infectious while the other is not, as in the case of TB and diabetes. Either way, these syndemics adversely influence disease outcomes. Surveillance activities may consider these interactions. Finally, the role of social, structural and biological determinants of disease and death are rarely completely understood in terms of disease distribution or prevalence.

02 **Increasing rates of non-communicable diseases and acute and chronic conditions:** The Ministry of Health in its document "India – Health of Nation's

Anonymization Techniques

Anonymization models :

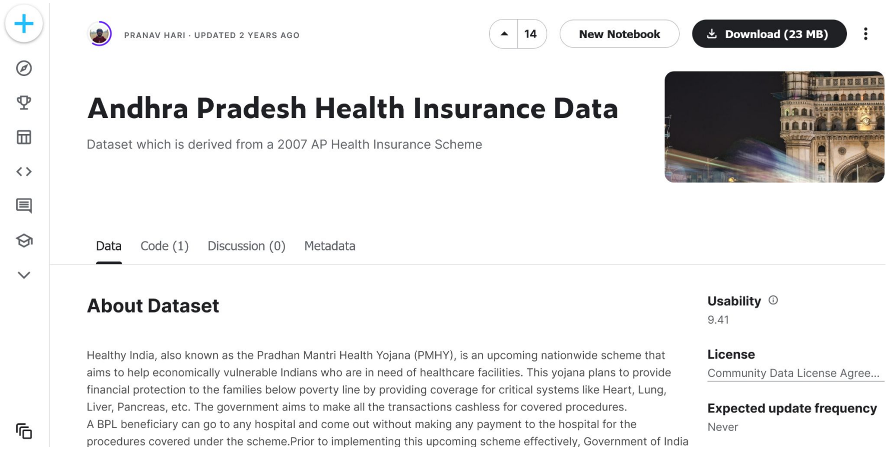
- ***k*-anonymity** : *k*-anonymity requires that at least *k* individuals share the same attributes. Since QID contains fields that are likely to appear in other known datasets, *k*-anonymity ensures that each individual remains anonymous within their respective group (equivalence class).
- ***l*-diversity** : *l*-diversity overcomes the limitations of k-anonymity by considering diversity among SAs. *l*-diversity ensures that there are at least *l*-distinct values of SA in each equivalence class.
- ***t*-closeness** : *t*-closeness ensures that the distance between the distribution of sensitive values in each equivalence class and the original class is no more than a threshold *t*. Hence, a smaller value of *t* represents stronger privacy.

Attacks on Anonymization

- **Knowledge attacks** : When an adversary knows some information or QIDs about the target individual, she can reconstruct the identifiable information of the individual.
- **Linkage attacks** : One where an adversary can re-identify or link a record in an anonymized dataset by combining QIDs from different sources to an individual.
- **Attribute disclosure attacks** : The attacker aims to gain new information on SA. The attacker can also exploit the properties of the QIDs to estimate the SA.
- **Membership disclosure attacks** : Involves an adversary aiming to infer the presence or absence of an individual in a dataset.

Example of badly anonymized dataset

- **56** **Female** **BC** M6 NEPHROLOGY M6.5 **Maintenance Hemodialysis For Crf Lolugu** **Ponduru** **Srikakulam** 03-08-2013 20:38 **12,500** 22-03-2017 20:25 11,000 **Rims Govt. General Hospital, Srikakulam** G Srikakulam **06-08-2013 00:00 (DOS)** **07-09-2013 00:00 (DOD)** **NO** D



Andhra Pradesh Health Insurance Data

Dataset which is derived from a 2007 AP Health Insurance Scheme

About Dataset

Healthy India, also known as the Pradhan Mantri Health Yojana (PMHY), is an upcoming nationwide scheme that aims to help economically vulnerable Indians who are in need of healthcare facilities. This yojana plans to provide financial protection to the families below poverty line by providing coverage for critical systems like Heart, Lung, Liver, Pancreas, etc. The government aims to make all the transactions cashless for covered procedures.
A BPL beneficiary can go to any hospital and come out without making any payment to the hospital for the procedures covered under the scheme.Prior to implementing this upcoming scheme effectively, Government of India

Usability
9.41

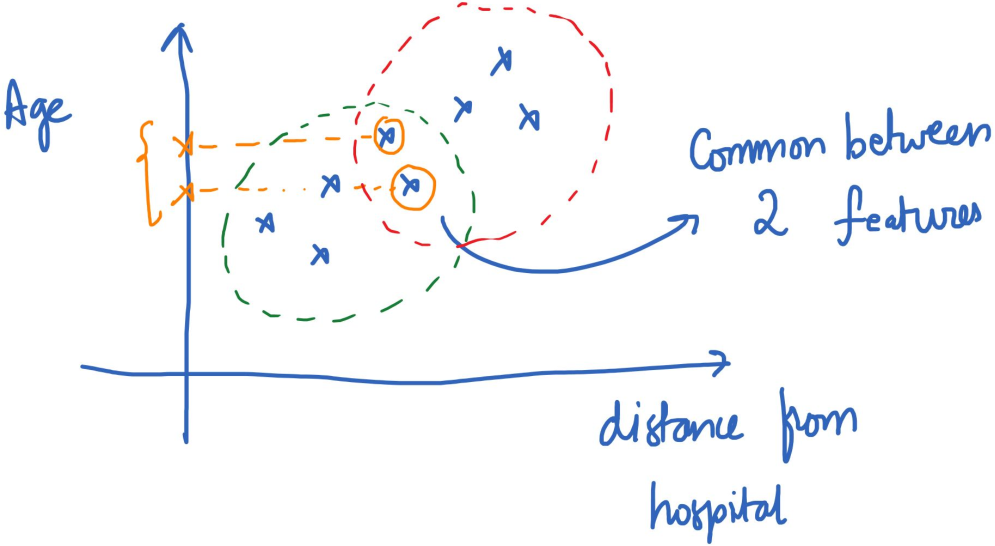
License
Community Data License Agree...

Expected update frequency
Never

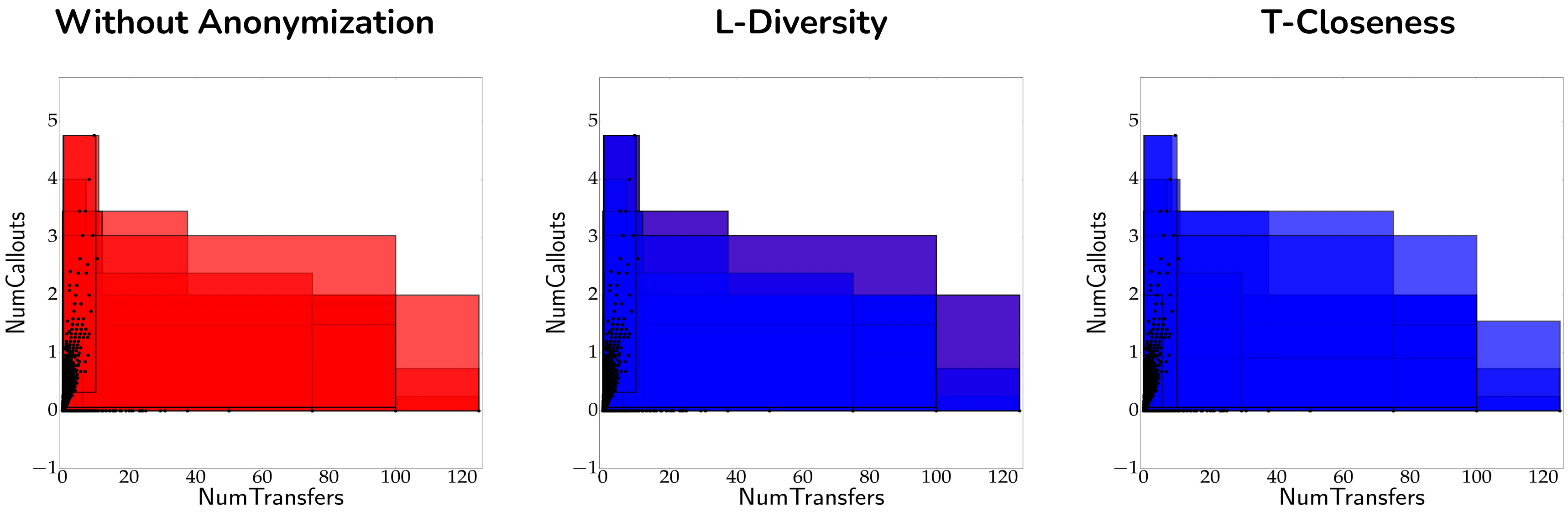
Dataset and Method

- MIMIC-III is a large, freely-available database comprising de-identified health-related data associated with over 40,000 patients who stayed in critical care units of the Beth Israel Deaconess Medical Center between 2001 & 2012
- We created a dummy task of predicting the LOS (Length of Stay) Group in the given dataset based on different features available
- Some of the columns available in the dataset are **admit_type, admit_location, Number of callouts** etc. apart from general details of the patient like **gender**, **age**, **religion,** etc
- Method used for K-Anonymizing the data - **Mondrian Algorithm,** followed by **L-diversity** and **T-closeness**

Dataset and Method



Experiments & Results



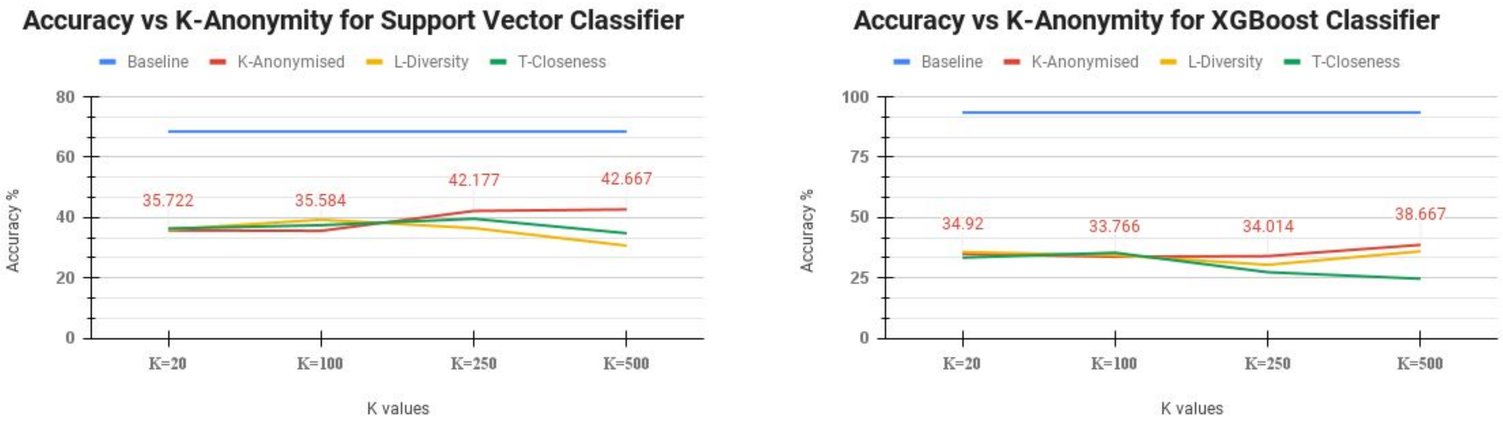
Without Anonymization

L-Diversity

T-Closeness

Fig. Mondrian Plots for different Anonymization Algorithms

Experiments & Results (Contd.)



Accuracy vs K-Anonymity for Support Vector Classifier

Accuracy vs K-Anonymity for XGBoost Classifier

Fig. The Trade-Off between Accuracy and Anonymization

Conclusion

- In this project, we provided a comprehensive review of anonymization models and techniques applicable for health care data
- Emphasis of deanonymization of data was provided along with a detailed explanation of the K-Anonymity method of deanonymization
- Demonstrated the effect of anonymization on ML model training and showed that accuracy decreases with stricter anonymization

Recommendations

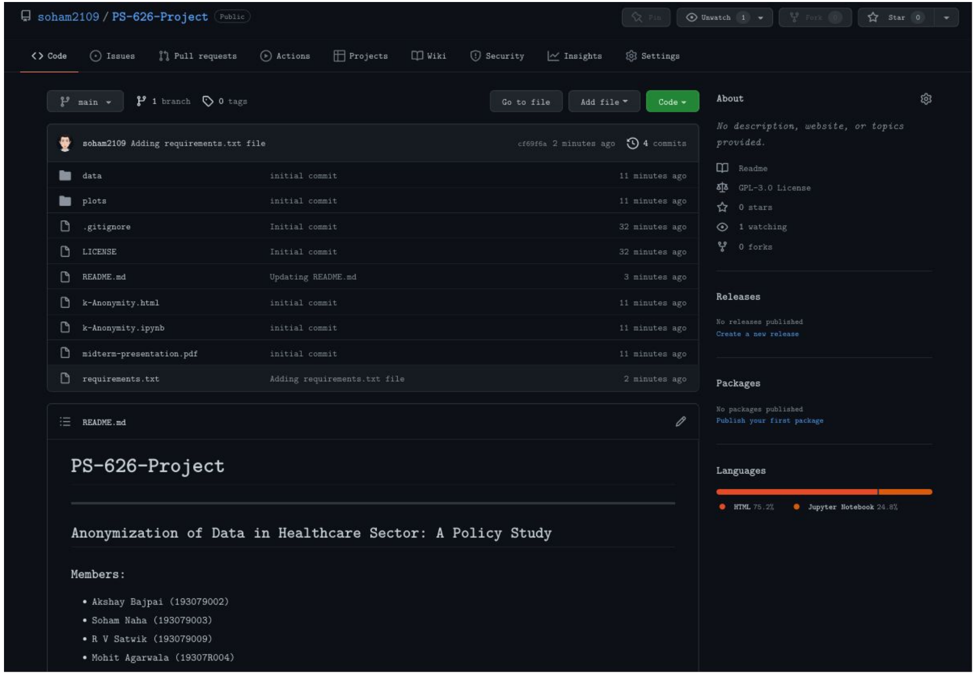
- Given the tradeoff between the accuracy of an algorithm and the amount of deanonymization, it becomes imperative for the government to propose proper guidelines on the metrics or scores used for measuring deanonymization (such as commonality between features)
- Further, any data made public must adhere to the said threshold or recommendation in order to avoid loss of privacy of the citizens whose data has been collected/stored

Recommendations (future work)

- The policy must provide a guideline on the size of dataset needed for an application based on the complexity of the model. This ensures that only representative data required is shared instead of placing the entire data at risk
- The policy must also suggest the time span to which the data can be stored and the accountability in case the data has to be stored indefinitely for training of models

Code Links

https://github.com/soham2109/PS-626-Project/



soham2109 Adding requirements.txt file cf69f6a 2 minutes ago 4 commits

data	initial commit	11 minutes ago
plots	initial commit	11 minutes ago
.gitignore	Initial commit	32 minutes ago
LICENSE	Initial commit	32 minutes ago
README.md	Updating README.md	3 minutes ago
k-Anonymity.html	initial commit	11 minutes ago
k-Anonymity.ipynb	initial commit	11 minutes ago
midterm-presentation.pdf	initial commit	11 minutes ago
requirements.txt	Adding requirements.txt file	2 minutes ago

README.md

PS-626-Project

Anonymization of Data in Healthcare Sector: A Policy Study

Members:

- Akshay Bajpai (193079002)
- Soham Naha (193079003)
- R V Satwik (193079009)
- Mohit Agarwala (19307R004)

About

No description, website, or topics provided.

Readme
GPL-3.0 License
0 stars
1 watching
0 forks

Releases

No releases published
Create a new release

Packages

No packages published
Publish your first package

Languages

● HTML 75.2% ● Jupyter Notebook 24.8%

References

- Broken Promises of Privacy
- 'Data is a fingerprint': why you aren't as anonymous as you think online
- De-Health: All Your Online Health Information Are Belong to Us
- Your Data Were ‘Anonymized’? These Scientists Can Still Identify You
- Anonymization of General Practioner Medical Records
- Data re-identification (Wikipedia)
- De-Identifying Medical Patient Data Doesn’t Protect Our Privacy
- Personal data anonymization
- Protecting Privacy Using k-Anonymity
- Vision 2035: Public Health Surveillance in India: A White Paper

Thank you