Enhancing a Solidarity-Based Approach to Health Data

Defining health data and principles for its use:

Focus:

> *This is about the issue of balancing privacy and solidarity in the use of data for public health. Some things about COVID-19 contact tracing apps. Broadly, proposals for how to classify health data, and make sure that health data has an additional layer of protection and at the same time can be used to support decision making.*

Key Takeaways:

- COVID-19 tracing apps must be locally adapted and consider key principles of privacy. Several important recommendations include i) anonymity, ii) transparency, iii) deletion of data after appropriate time period, and iv) privacy-centred design.
- Regional and national policies which attempt to regulate and define the use of health data often appear broad. There is often emphasis on data sharing, which demonstrates its importance and need for regulatory priority due to its intersection with free market potentials, but there is less specificity on what these means to the individual. Notably most of this regulation has a judicial origin.

1. **Tracking and Tracing COVD: protecting privacy and data while using apps and biometrics. OECD 2020. Source.**

Key Topics: Coordination; Cooperation; Data sharing; COVID-19; Tracing

Source Type: Policy response

Focus: Global governance policy for national implementation

Case Made:

The COVID-19 pandemic has seen an unprecedented amount of the use of digital technologies to improve health care. Simultaneously, the rise of the digital in the health space has often outpaced the capacity of governments' regulations. This has raised concerns over COVID-19 data privacy.

Solutions Suggested or Implemented:

"Fully transparent and accountable privacy-preserving solutions should be embedded by design to balance the benefits and the risks associated with personal data collection, process and sharing. Data should be retained only for so long as is necessary to serve the specific purpose for which it was collected."

Key topics for consideration when collecting data:

"Contact-tracing apps should be implemented with full transparency, in consultation with major stakeholders, robust privacy-by-design protections, and through open source projects (where appropriate). Governments should consider:

- The legal basis of the use of these technologies, which varies according to the type of data collected (e.g. personal, sensitive, pseudonymised, anonymised, aggregated, structured or unstructured).
- Whether the use of these technologies and the subsequent data gathering is proportionate, and consider how the data is stored, processed, shared and with whom (including what security and privacy-by-design protocols are implemented).
- The quality of the data collected and whether it is fit for purpose.
- Whether the public is well-informed and the approaches adopted are implemented with full transparency and accountability.
- The time period within which more invasive technologies that collect personal data may be used to combat the crisis. Data should be retained only for so long as is necessary to serve the specific purpose for which it was collected."

In practice, consider mechanisms to build in privacy by design, the following is an explanation of the concept and several examples of its successful implementation:

"**Privacy-by-design** seeks to deliver the maximum degree of privacy by ensuring that personal data protections are built into the system, by default. Privacy-by-design may, for example, involve the use of aggregated, anonymised, or pseudonymous data to provide added privacy protection, or the deletion of data once its purpose is served.

For instance, the COVID-19 app developed by the Norwegian Institute of Public Health is designed to store location data only for 30 days. The use of additional privacy enhancing solutions (such as homomorphic encryption)1 may provide added security, as can the use of data sandboxes, through which access to highly sensitive (personal) data is only granted within a restricted digital and/or physical environment to trusted users. An example of the latter is Flowminder, which collaborated with telecommunication companies during the 2014-16 Ebola outbreak to provide epidemiologists with secured access to de-identified low-resolution geolocation data. Flowminder is using a similar strategy in contributing to the response to the COVID-19 crisis.

The use of geolocation data-collecting apps can allow data-sharing with explicit, built-in privacy and data protections, and enable users to give their explicit, informed consent to the collection and sharing of their personal data (assuming use of the app is not mandatory). For instance, Singapore's TraceTogether app has a number of privacy safeguards, including that it does not collect or use geolocation data and data logs are stored in an encrypted form. To protect the privacy of its users, the Pan-European app encrypts data and anonymises personal information.

In addition, as two phones never exchange data directly and the users' aliases are changed frequently, it is virtually impossible to reveal the identity of users.

However, the range of personal data these apps collect, process and share can be very broad and difficult for users to understand. In many cases, apps continue to run in the background even when the device is not in use. Some apps can also exchange information with other apps through application programming interfaces (APIs), generating more detailed information. While the World Health Organization (WHO) praised Korea's extensive tracing measures, some uses by designated local authorities of the data collected through the Epidemiological Investigation Support System on the movements of persons with confirmed cases have raised privacy concerns. In response, the Korean government recently published guidance related to the disclosure of the movements of persons with confirmed cases based on the Infectious Disease Control and Prevention Act passed in 2015 which does not allow any information specific to the data subject to be disclosed.

The use of biometrics (including facial recognition) in response to COVID-19 raises a number of privacy and security concerns, particularly when these technologies are being used in the absence of specific guidance or fully informed and explicit consent. Individuals may also have problems exercising a wide range of fundamental rights, including the right of access to their personal data, the right to erasure, and the right to be informed as to the purposes of processing and who that data is shared with. Facial recognition systems can also have inherent technological bias, e.g. when based on race or ethnic origin."

2. **Principles of the GDPR. European Union. 2021. Source.**

Key Topics: GDPR; EU; Data; Privacy; Regulation; Personal

Source Type: European Union Regulations

Focus: Regional (Europe)

Case Made:

Solutions Suggested or Implemented:

The GDPR operates on a level of interesting ambivalence when considering *what type* of data is to be protected. Broadly, this is defined as "personal data." However, this term is very flexible, and does not hold a consistent definition, likely allowing itself to be adapted within different country contexts.

Regulations for the Private Sector:

- Data must be collected and processed transparently, for specific purposes, and no data can be collected beyond the needed data for each use case.

Rights provided to individuals:

- User has the right to ask for any data of theirs being used by a company, receive a copy, request that personal data be erased, request the restriction of processing of that data, and or prohibit the automated processing of personal data.
- For restrictions to be placed on personal data, it will often need to meet criteria including: personal data is being used for direct marketing, personal data is being used for scientific/historical research and statistic, and or for the individual's own legitimate interest. In the most latter case, a burden of proof can be placed upon the company to override the individual's claim and "therefore a balancing act is required."

3. The Role of Indian Data for European AI. Bertlesmann Stiftung. 2020. Source.

Key Topics: Data; Data sharing; Regulation; Judiciary; Legislation; Security; Implementation; Personal; Non-personal

Source Type: Private sector market and governance report

Focus: National (India)

Case Made:

This report reviews existing regulation and oversight of data for the purpose of considering how data can be shared, sold, and used for collaboration between the EU (specifically Germany) and India.

Solutions Suggested or Implemented:

Perhaps the most useful take away for the Report in this source is how the EU governs only "personal data" whereas Indian data governs both "personal and non-personal" information. Similarly between contexts, definitions of these terms is largely lacking which may be another area that can be addressed by the Report.

The following is an overview of how health data is governed, mostly through creation in the judiciary, and as well as regulatory oversight, implementation and security:

India is in a phase of transition with regards to its privacy and data protection principles and laws. A landmark judgement by the country's Supreme Court in August 2017 recognized the right to privacy as a fundamental right under Article 21 of the Constitution as a part of the right to "life" and "personal liberty." "Informational privacy" has been recognized as a facet of the right to privacy, where privacy protection extends to information about a person and the right to access that information.87 Thus, India has effectively enshrined privacy as a fundamental right, something that has far-reaching positive consequences for its future activities in the area of data

privacy and the secure exchange of data. As mentioned, in 2017, India drafted a Personal Data Protection (PDP) bill, which is currently being discussed in parliament.

India does not yet have a dedicated data protection law, and data in the country is protected by the Information Technology Act from the year 2000 and by the IT Rules from 2011, which are particularly relevant for data protection and cross-border transfers.88 The IT Rules of 2011 in combination with the IT Act lay down that corporations must possess a comprehensive privacy policy for handling personal information (Rule 4) and obtain the provider's consent before collecting personal information for a purpose connected with its own functions (Rule 5).89 For disclosure of information to a third party,90 the permission of the provider must be in the contract itself. Otherwise the third party cannot disclose this information further. Section 7 gives adequacy provisions for cross-border movement of data.91 Section 43A ensures reasonable data safety procedures by providing for compensation in case of a failure to protect data.92 Section 72A93 applies to contraventions committed in and outside94 India irrespective of nationality and penalizes disclosure of personal information without consent.

Implementation and enforcement gaps as well as data security leaks suggest that:

"Given this evidence, it seems clear that neither the current legal base for data protection in India (IT Act) nor the data privacy practices observed among stakeholders provide comprehensive protection for personal data. While strong implementation of the PDP bill and establishment of a DPA promise considerably higher levels of data protection in the country, the decision to promote a data partnership for AI between Germany/EU and India needs to consider these realities."

Building data institutions for data solidarity in health:

Focus:

> *Beyond the balance between health and data above, this has to do with the type of institutions you set up. This can have a lot to do with trust. Here there is not a lot on the global.*

Key Takeaways:

- From the searches in this research, there was little found on country level approaches. More has been revealed on this topic on the global governance and conceptual level.
- Global governance broadly reaffirms the need to balance the potential of health data and the need for data privacy and rights.
- On the conceptual level, there is discussion about ways to provide data 'firewalls' which prevents data use by governments to use data for predatory means (i.e. police). Key words which might be useful for the report are 'smart governance' and 'adaptable governance.'
- In sum, both global governance and academics agree that there is a need to approach this issue through the lens of safeguarding rights and keeping government institutions adaptable for rapid changes in the technology space.

1. Health Data Governance: Privacy, Monitoring and Research. OECD. 2015. Source.

Key Topics: UHC, Data solidarity; Data rights; Fundamental infrastructures

Source Type: Report

Focus: Global

Case Made:

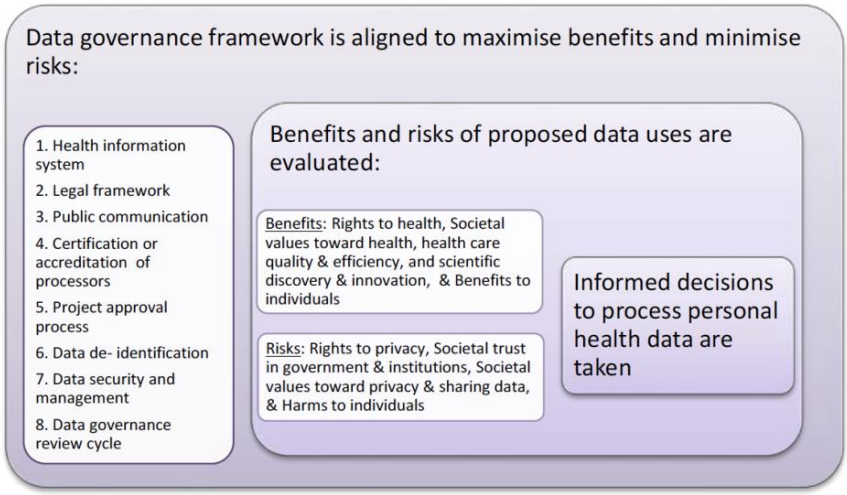
The OECD suggests that it is important to be more attuned to how data solidarity can work towards UHC. without health data sharing countries will not be able to accomplish increased access, quality, and research for health.

Solution Suggested or Implemented:

The report begins by providing an explanation of how data solidarity can work to accomplish UHC, specifically that. For this report, the goals of health data should be to track patient outcomes across all levels of the health system, as well as to ensure the comparability of these results.

The report recommends a framework which aims to balance societal and individual risks and benefits:

Figure 3. Data use decisions should be taken by weighing societal benefits and risks within a data governance framework that maximises benefits and minimise risks



The report concludes with 8 recommendations:

i) The health information system supports the monitoring and improvement of health care quality and system performance, as well as research innovations for better health care and outcomes.

ii) The processing and the secondary use of data for public health, research and statistical purposes are permitted, subject to safeguards specified in the legislative framework for data protection.

iii) The public are consulted upon and informed about the collection and processing of personal health data.

iv) A certification/accreditation process for the processing of health data for research and statistics is implemented.

v) The project approval process is fair and transparent and decision making is supported by an independent, multidisciplinary project review body.

vi) Best practices in data de-identification are applied to protect patient data privacy.

vii) Best practices in data security and management are applied to reduce re-identification and breach risks.

viii) Governance mechanisms are periodically reviewed at an international level to maximize societal benefits and minimize societal risks as new data sources and new technologies are introduced.

2. **A Call to Action for Health Data Governance. Lawrence Gostin & Effy Vayena. World Health Summit. 2020. Source: NFF.**

Key Topics: Data use; Trust; Privacy; Solidarity; IHR

Source Type: Event

Focus: Global

Case Made:

Specifically within the context of COVID-19, data on individual health is needed to make useful population policies. However, when individual health data is used by the government, it can also be reappropriated for predatory purposes (i.e. the police). Better governance is needed.

Solution Suggested or Implemented:

When speaking about how to balance data privacy and public health, Lawrence suggested the idea of smart law and smart governance. This involves (non-traditional) governance mechanisms which earmark collected data for the uses exclusively of public health officials, and firewalled to other government agencies such as the police. This aims to look for the in-betweens of leaving it to the consumer and being authoritarian.

Another participant, Effy, spoke about adaptable governance in addition to this. This builds on smart law and smart governance by suggesting that these practices will need to be changed frequently. Effy suggests that this will help to continue to build public trust.

Both Effy and Lawrence suggested that one of the most practical ways forward to balance data privacy and public health would be through modifying the IHR. However, Lawrence cautioned that within the current political climate the IHR should not be opened up as a whole, but for now these considerations should be done within the IHR annex.