PAPER 4

DIGITAL TECHNOLOGY, HEALTH & THE LAW
Implications for UHC

Centre for Health Equity, Law & Policy, ILS Pune

Prepared for the Governance Workstream of the
Lancet Citizen's Commission on Reimagining India's Health System

C-HELP
CENTRE FOR HEALTH EQUITY, LAW & POLICY

ILS®

CONTENTS

List of abbreviations

ABDM	Ayushman Bharat Health Mission
ABHA	Ayushman Bharat Health Account
AB-HWC	Ayushman Bharat Health and Wellness Centre
AI	Artificial intelligence
API	Application Programming Interface
AYUSH	Ayurveda, Yoga and Naturopathy, Unani, Siddha and Homeopathy
BI&A	Business Intelligence and Analytics
CAGR	Compound Annual Growth Rate
CoWIN	COVID-19 Vaccination Intelligence Network
EHR	Electronic health record
EU	European Union
GDPR	General Data Protection Regulation
GPS	Global Positioning System
HDMP	National Digital Health Mission: Health Data Management Policy
HIS	Health information system
HTA	Health technology assessment
ICCPR	International Covenant for Civil and Political Rights
IoT	Internet of Things
JPC	Joint Parliamentary Committee
MeitY	Ministry of Electronics and Information Technology
MoHFW	Ministry of Health and Family Welfare
ICESCR	International Covenant for Economic, Social and Cultural Rights
NFHS	National Family Health Survey
NHA	National Health Authority
NDHM	National Digital Health Mission
NDHM-GRO	NDHM Grievance Redress Officer
NeGD	National e-Governance Division

NeGP	National e-Governance Plan
NFHS	National Family Health Survey
NICE	National Institute for Health and Care Excellence
NSSO	National Sample Survey Organisation
OHCHR	Office of the High Commissioner for Human Rights
PbD	Privacy by design
PII	Personally identifiable information
RMP	Registered medical practitioner
UHC	Universal health coverage
UN	United Nations
UNDP	United Nations Development Program
UNGA	United Nations General Assembly
UNHRC	United Nations Human Rights Commissioner
WHA	World Health Assembly
WHO	World Health Organisation

INTRODUCTION

Normative guidance in international human rights law embeds digital health in international human rights and ethical frameworks to minimise the harms associated with digitalization. It is globally recognised that while there is utility in using digital health technologies for universal health coverage (UHC), this deployment must be embedded in respect for human rights, ethics and equity, and maintain acceptable quality, safety and ethical standards. This is most clearly articulated in the 'Political declaration of the high-level meeting on universal health coverage' passed by the United Nations General Assembly (UNGA) in 2019. The declaration recognises that digital health technologies must yield to the needs of privacy and equity rights in relation to data collection, and narrow the digital divide while promoting health priorities.[1]

It is widely believed that digital technologies offer opportunities to support health systems especially in low- and middle-income countries right from patient information collection, diagnostics and remote clinical monitoring to supply-chain management and disease surveillance. In March 2023, a World Health Organisation (WHO) conference, 'Taking UHC to the last citizen', was held in New Delhi, calling for harnessing digital technologies to accelerate progress towards UHC. India's minister for health elaborated on India's approach to adopting digital health tools for achieving UHC thus: "*India has adopted a two-pronged approach with a focus on digital health through a policy framework and by creating a digital ecosystem for path breaking interventions which focus on not just availability, accessibility, affordability but also equity of health services.*"[2]

While promoting the use of digital health as instrumental in achieving UHC, the WHO has consistently acknowledged that it also poses significant harms to rights and freedoms. This is documented in the World Health Assembly (WHA) resolutions on eHealth in 2005[3] and digital health in 2018[4], as well as WHO's global strategy for digital health (2020–2025)[5] and manual on Electronic Health Records (EHR).[6] The WHO has repeatedly emphasised three prerequisites for a responsible transition to digital health that would enable the full harnessing of its potential and minimise associated harms: (a) develop a comprehensive data protection law which regulates all processes related to data and protects the rights to consent, confidentiality, privacy and inclusivity consistent with international human rights obligations and ethical principles, as well as safeguards individual health data from unauthorised access, abuse and theft; (b) build institutional capacity to effectively regulate all processes related to data; and (c) ensure health system capacity and preparedness by assessing and improving healthcare documentation, accuracy of data, infrastructural capabilities, human resources and training requirements, quality control and cybersecurity governance.

Notably, the global strategy for digital health (2020-2025) places digital health within the larger need for delivering on social determinants of health, and recognises that *"digital determinants of health*

---

[1] UNGA Resolution, Political Declaration of the High-level Meeting on Universal Health Coverage "Universal health coverage: moving together to build a healthier world", 2019. Available at: https://www.un.org/pga/73/wp-content/uploads/sites/53/2019/07/FINAL-draft-UHC-Political-Declaration.pdf.

[2] WHO (2023). Harness digital health for Universal Health Coverage. World Health Organisation. Available at: https://www.who.int/southeastasia/news/detail/20-03-2023-harness-digital-health-for-universal-health-coverage.

[3] World Health Assembly Resolutions on ehealth in 2005. Available at: https://apps.who.int/iris/handle/10665/20398.

[4] World Health Assembly Resolution on Digital health. 26 May 2018. Available at: https://apps.who.int/gb/ebwha/pdf_files/WHA71/A71_R7-en.pdf.

[5] WHO (2021). Global Strategy on Digital health (2020 – 2025). Available at: https://www.who.int/docs/default-source/documents/gs4dhdaa2a9f352b0445bafbc79ca799dce4d.pdf.

[6] Electronic Health Records: Manual for Developing Countries. World Health Organisation. Available at: https://apps.who.int/iris/bitstream/handle/10665/207504/9290612177_eng.pdf?sequence=1 .

such as literacy in information and communication technologies and access to equipment, broadband and internet, becomes more important as digital health becomes more prevalent."[7]

When the world was confronted with COVID-19 in 2020, the WHA recognised the need to leverage digital health technologies but to do so by "*paying particular attention to digital inclusion, patient empowerment, data privacy, and security, legal and ethical issues, and the protection of personal data.*"[8] Shortly thereafter, the UNGA adopted a resolution that encouraged the use of digital technologies to combat COVID-19, while "*adhering to the objectives of efficacy, safety, equity, accessibility, and affordability.*"[9] Conscious of the deployment of digital surveillance measures to respond to COVID-19, the United Nations Secretary-General stated that protection of human rights must be central to the COVID-19 response.[10] In 2020, the UN special rapporteur on the right to privacy warned that invasive digital surveillance could "*cause lasting damage to the right to privacy…[d]ictatorships and authoritarian societies often start in the face of a threat.*"[11]

The objective of this paper is to critically examine the policy and proposed legal framework governing digital health technologies in India, as well as the deployment of digital health tools – EHRs, telemedicine, digital disease surveillance, artificial intelligence (AI) applications and digital vaccine management – as against the obligations under human rights and ethics frameworks. The analysis reveals the extent to and the manner in which individuals are protected against the potential harms associated with digital health technologies being deployed by central and state governments as well as private entities in India. The ramifications are considerable for the roll-out of UHC, given the inevitable use of digital health technologies in any such conception.

Section 1 of this paper explains why the deployment of digital health technologies and its governance must be anchored in the international human rights framework – particularly, the rights to privacy and health - as well as the ethical frameworks, which are also firmly part of Indian law. The right to privacy and the right to health, which also includes privacy concerns, are explicitly coded in international human rights law. The right to privacy can be interfered with only when there is a legitimate purpose, necessary for achieving that purpose, proportionate to the objective and must be the least intrusive means of restriction. The other relevant rights component – the right to health framework – is also expounded on, which recognises that digital health technologies must be implemented in an accessible and acceptable manner, be available to all, and be of reasonable quality that advances the right to health while not hindering it.

Section 2 applies the international human rights law framework and ethics to critically analyse the adoption of digital health policies and deployment of digital health tools in India. Section 3 discusses the legal ethical issues arising from the use of AI in the health sector and its implications for UHC and the right to health. Section 4 discusses growing data monetisation, leveraged by big data analytics and AI, by Big Tech companies and in the health insurance and pharmaceutical sector, and its impact on UHC and the right to health. Section 5 critically examines the proposed legislative frameworks in India

---

[7] WHO (2021). Global Strategy on Digital health (2020 – 2025). Available at: https://www.who.int/docs/default-source/documents/gs4dhdaa2a9f352b0445bafbc79ca799dce4d.pdf.

[8] WHA (2020). COVID-19 Response. WHA 73.1. Available at: https://apps.who.int/gb/ebwha/pdf_files/WHA73-REC1/A73_REC1-en.pdf#page=1.

[9] UNGA (2020). Comprehensive and coordinated response to the coronavirus (COVID-19) disease pandemic. A/74/L.92. Available at: https://documents-dds-ny.un.org/doc/UNDOC/LTD/N20/231/11/PDF/N2023111.pdf?OpenElement.

[10] Guterres, Antonio (2020). We are all in this Together: Human Rights and COVID-19 Response and Recovery. United Nations. Available at: https://www.un.org/en/un-coronavirus-communications-team/we-are-all-together-human-rights-and-covid-19-response-and.

[11] Bacchi, Umberto (2020). Coronavirus surveillance poses long-term security threat. Reuters. Available at: https://in.reuters.com/article/health-coronavirus-privacy/coronavirus-surveillance-poses-long-term-privacy-threat-u-n-expert-warns-idINKBN21I1WU

for regulating the use of personal and non-personal data, in context of the international and constitutional law, and globally established privacy and data protection standards, and whether these provide adequate protection from risks and harms discussed in the preceding sections. Section 6 concludes with key recommendations.

1 DIGITAL HEALTH, INTERNATIONAL HUMAN RIGHTS AND ETHICS FRAMEWORKS

1.1 Digital Health must be anchored in human rights and ethical frameworks

Digital health tools and technologies[12] have been heralded as a "*critical solution to challenges and gaps in the delivery of quality health care.*"[13] They are regarded as essential for Universal Health Care (UHC), as an enabler of increasing availability and accessibility of quality health services, which are essential elements of the right to health.[14] Yet, they also present risks of violation of autonomy, privacy and confidentiality of sensitive health data, which can in turn lead to violations of a host of other rights, including the rights to health, inclusion and non-discrimination, employment, freedom of assembly and expression and protection from arbitrary detention.[15]

It is, therefore, essential to embed digital health in a rights-based approach, and build the health system's regulatory and institutional capacity for governing the use of technology in a way that supports and strengthens health delivery while protecting rights, particularly the rights related to health, privacy and equality and non-discrimination.

1.2 Risks of digitalisation in health – impact on a range of human rights

The extent to and manner in which technology can aid in improving the availability and accessibility of health services will vary from place to place. At the same time, technology presents risks that can hinder the full realisation of the right to health; and implementation of any technological solution must be cognizant of those risks.

1.2.1 Risk of data breaches and unauthorised disclosure of sensitive health data

Data breaches have a variety of causes, from malware and ransomware to accidental or purposeful disclosure. In the last few years, there have been several instances of hacking,[16] leak of health data[17] as well as unauthorised disclosure by the government of personal health data of individuals affected by COVID-19.[18]

According to a Data Security Council of India (DSCI) report, India suffered the second most cyber-attacks between 2016 and 2018.[19] Digital health data is particularly targeted as data security remains

---

[12] Digital health is referred to as "*a broad umbrella term encompassing eHealth (which includes mHealth and telemedicine), as well as emerging areas, such as the use of advanced computing sciences in 'big data', genomics and artificial intelligence.*" World Health Organisation (WHO) (2019). *Guidelines on 'Recommendations on Digital Health Interventions for Health System Strengthening'.* Available at: https://apps.who.int/iris/bitstream/handle/10665/311941/9789241550505-eng.pdf?ua=1

[13] Sun, N. et al. (2020). Human Rights and Digital Health Technologies. Health Hum Rights. Dec;22(2):21-32. PMID: 33390689; PMCID: PMC7762914.

[14] Supra at 11

[15] Supra at 2

[16] Indo-Asian News Service (2019, August 22). *Hackers attack Indian healthcare website, steal 68 lakh records.* India Today. Available at: https://www.indiatoday.in/crime/story/hackers-attack-indian-healthcare-website-steal-68-lakh-records-1590345-2019-08-22

[17] *Healthcare Data Leak: Over 120 Mn Medical Images of Indian Patients Left Exposed.* 2020, February 4. Inc42.com. Available at: https://inc42.com/buzz/india-healthcare-data-leak-over-120-mn-medical-images-exposed/; *In major error, millions of pregnant women's data leaked online.* 2019, April 9. Health Issues India. Available at: https://www.healthissuesindia.com/2019/04/02/in-major-error-millions-of-pregnant-womens-data-leaked-online/; *Data, Privacy, Pandemic: India just had the biggest medical record breach ever.* Observer Research Foundation. 2021, January 12. Available at: https://www.orfonline.org/expert-speak/data-privacy-pandemic-india-just-had-the-biggest-medical-records-breach-ever/

[18] *Why Reveal Names of COVID-19 Patients? It Involves Privacy: High Court Seeks Government's Reply.* 2020, July 10. NDTV. Available at: https://www.ndtv.com/india-news/why-reveal-names-of-covid-19-patients-it-involves-privacy-high-court-seeks-governments-reply-2260413

[19] India Second Most Affected Country Due to Cyber Attacks. 2019, May 3. Inc42.com. Available at: https://inc42.com/buzz/cyber-attacks-india/

weak in this sector.[20] Stolen health data is sold on the darknet and is used for identity theft, fraudulent billing[21] and blackmail.[22] In the recent ransomware attack on AIIMS, hackers stole health data of more than 30 million patients and encrypted the records which rendered them inaccessible for 14 days.[23] This, along with jeopardising patient privacy also delayed care, which could have life threatening consequences.

The consequences of leaked healthcare data could expose an individual to embarrassment, stigma, isolation, ostracisation, discrimination and potentially violence, from others who may hold discriminatory attitudes towards certain health conditions, such as HIV, STIs, mental health conditions, abortions etc. For instance, in May 2021, the Insurance Regulatory and Development Authority of India warned insurers against using leaked personal health records of COVID-19 patients to deny insurance coverage or block claims by policyholders.[24] Leaked healthcare data containing sensitive personal data such as an abortion or a sexually transmitted disease can expose vulnerable populations to all kinds of mental and physical harassment at home and in public places. On a large scale, it can put countries at the risk of biological warfare.[25]

1.2.2 Risk of state surveillance and function creep

The 2017 Report by the Committee of Experts under the Chairmanship of Justice B.N. Srikrishna[26] and the *Puttaswamy* judgment in the same year, warned of the risk of state surveillance in the era of digitalisation and the need to guard against it. Electronic health records (EHRs), even if determined to be necessary, have been described as 'privacy-invasive tools of eHealth'.[27] The UNAIDS Guidance Document for adoption of EHRs cautions against the dangers of having an EHR system compromised or inappropriately used or accessed to track individuals by both state and non-state actors.[28] The use of Aadhaar to create digital health IDs, as was done at the time of COVID-19 vaccination drives, will link EHR data with other data sources, beyond healthcare and will enable the State to build profiles of individuals through the convergence of data. This entails risks of misuse of personal information for unauthorised surveillance and censorship, which in addition to infringing privacy will impact civil liberties more broadly and undermine democracy. For instance, an Andhra Pradesh Assembly

[20] Koppel, R. & Kuziemsky, C. (2019). Healthcare Data Are Remarkably Vulnerable to Hacking: Connected Healthcare Delivery Increases the Risks. Stud Health Technol Inform.
[21] Schlesinger, J. & Day A. (2016, March 11). Dark Web is fertile ground for stolen medical records. CNBC. Available at:https://www.cnbc.com/2016/03/10/dark-web-is-fertile-ground-for-stolen-medical-records.html; Lord, R. (2017, December 15). *The Real Threat Of Identity Theft Is In Your Medical Records, Not Credit Cards.* Forbes. Available at: https://www.forbes.com/sites/forbestechcouncil/2017/12/15/the-real-threat-of-identity-theft-is-in-your-medical-records-not-credit-cards/?sh=52115b001b59
[22] Zorz, Z. (2020, October 26). *Hackers breach psychotherapy center, use stolen health data to blackmail patients.* Help Net Security. Available at: https://www.helpnetsecurity.com/2020/10/26/data-breach-psychotherapy-center/
[23] Sabarwal, H. (2022, December 14). *Delhi AIIMS ransomware attack carried out by hackers from China, Hong Kong: Report.* WION. Available at: https://www.wionews.com/india-news/attack-on-aiims-delhi-server-carried-out-by-chinese-hackers-report-543044
[24] Sengupta, D. & Shukla, S. (2021, May 13). *Covid-19 patients' health data being sold on dark web.* Economic Times. Available at: https://telecom.economictimes.indiatimes.com/news/privacy-fears-around-patients-health-data-breach-amid-covid-surge/82600300
[25] Mahajan, U. (2021). Role of Internet of Things in Biological Warfare. CBW Magazine (January-June 2021) Volume 14, Issue 2. Available at: https://idsa.in/cbwmagazine/role-of-internet-of-things-in-biological-warfare.
[26] Committee of Experts chaired by Justice B.N. Srikrishna "A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians". Available at: https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf
[27] (eds. Soenens, E., Leys, M.) (2008): eHealth identity management in several types of welfare states in Europe. FIDIS Deliverable D4.11. www.FIDIS-project.eu
[28] UNAIDS (2014), Considerations and Guidance for Countries Adopting National Health Identifiers. Available at: https://www.unaids.org/sites/default/files/media_asset/JC2640_nationalhealthidentifiers_en.pdf

Committee found the state government guilty of mining personal information, through the *Seva mitra* mobile app, to target and influence 30 lakh voters.[29] (See section 2 for more discussion)

1.2.3 Risk of profiling and commercialisation by private entities[30]

Instances of non-consensual collection of sensitive health data, unauthorised sharing with third parties and targeted advertising abound in the private sector. As per a Privacy International study which looked at mental health apps, period trackers and healthy diet apps, "*The 'adtech' industry is contributing to undermining the right to health by supporting an ecosystem in which health data is commoditised, shared with and used by third parties for commercial purposes*."[31] In an infamous example, Target (a retail store in the United States) used algorithms which could analyse the shopping details of women to predict a "pregnancy score" and enable targeted advertising. Following a shopping trip to Target, a young girl's pregnancy got outed to her family, as Target sent pregnancy related advertising products to her house.[32] (See section 4 for more discussion)

1.2.4 Risk of discrimination and exclusion due to digital divide

Digital technologies can exclude persons who do not or are unable to use technology platforms, thereby ironically exacerbating gaps in access and availability of services. A recent WHO study in Europe found that "*people with poor health are among the ones struggling the most in accessing these tools.*"[33] Making delivery of services contingent on digital IDs also leads to exclusion. A report of the Office of the High Commissioner on Human Rights (OHCHR) asserts the existence of robust documentation of individuals and communities who are less likely to have ID, such as the poor and disadvantaged, women, older persons, and members of some occupational groups; and underscores the concern that *"One major concern linked to comprehensive digital identification systems is that these systems can themselves be sources of exclusion, contrary to their purpose."*[34] A woman in labour was turned away by her local hospital for not having an Aadhaar card and later passed away during delivery at home.[35] During the COVID-19 pandemic, the insistence on exclusive digital platforms for service delivery as well on an Aadhaar card led to exclusions and denial of services. (See Section 2 for more discussion)

1.2.5 Risk of bias and discrimination vis-a-vis Big Data and artificial intelligence

Within healthcare, studies examining applications of AI have demonstrated that algorithms do not provide equally accurate predictions of health outcomes across race, gender, or socio-economic status, primarily due to the bias and under representativeness in the data sets on which they are trained. The WHO Ethical Guidance on AI in Health states that AI systems may lead to bias and

---

[29] Dara, G. (2022, September 21). *TDP govt mined personal data, tried to misuse it: Andhra Pradesh assembly committee.* Times of India. Available at: https://timesofindia.indiatimes.com/city/vijayawada/tdp-govt-mined-personal-data-tried-to-misuse-it-andhra-panel/articleshow/94337425.cms

[30] Commercial surveillance is the business of collecting, analyzing, and profiting from information about people.

[31] Privacy International (2019). Your Mental Health Is For Sale. Available at: https://privacyinternational.org/sites/default/files/2019-09/Your%20mental%20health%20for%20sale%20-%20Privacy%20International.pdf

[32] Hill, K. (2012, February 16). *How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did.* Forbes. Available at:http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/

[33] WHO (2022). *Equity within digital health technology within the WHO European Region: a scoping review.* Available at: https://www.who.int/europe/publications/i/item/WHO-EURO-2022-6810-46576-67595

[34] Annual report of the United Nations High Commissioner for Human Rights. A/HRC/43/29. *Question of the realization of economic, social and cultural rights in all countries: the role of new technologies for the realization of economic, social and cultural rights.* para 33. Available at: https://www.ohchr.org/sites/default/files/HRBodies/HRC/RegularSessions/Session43/Documents/A_HRC_43_29.pdf

[35] Bhuvneshwari, S. (2022, November 4). *Turned away by Tumakuru govt hospital, mom & twin newborns die*. The Times of India. Available at: https://timesofindia.indiatimes.com/city/mysuru/turned-away-by-tumakuru-govt-hospitalmom-twin-newborns-die/articleshow/95287187.cms

discrimination, which may further entrench inequalities and exclude historically disadvantaged groups such as girls and women, ethnic minorities, elderly people, rural communities and other disadvantaged groups.[36] (See Section 3 for more discussion)

1.3 Digital health and the right to privacy

Article 17 of the International Convention on Civil and Political Rights (ICCPR) recognizes the right to privacy as a fundamental human right. The General Comment 16 on the right to privacy notes that gathering and holding personal information on computers and other devices by public authorities or private organisations needs to be regulated by law.[37] It emphasises the right of individuals to ascertain whether and what personal data is being stored, by which public authorities or private entities, and for what reason.

The ICCPR requires States to respect and ensure that these rights are available to all individuals without discrimination (Article 2(1)). Therefore, all States have a clear obligation to not only refrain from violating the rights but also take positive steps to protect their enjoyment. This includes taking adequate legislative and other measures. If the right to privacy has to be interfered with, such action must be for a *legitimate* purpose, *necessary* for achieving that purpose, *proportionate* to the objective and must be the *least intrusive* means of restriction.

In addition to the ICCPR, the right to privacy has also been recognised in a regional convention, the European Convention on Human Rights.[38] Additionally, the European Charter of Fundamental Rights also recognises the right to data protection specifically. It is a legally binding document within the European Union that sets out the fundamental rights and freedoms of individuals . Article 8 of the Charter states "*Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.*"[39]

1.3.1 Privacy and Data Protection Legislation

The increase in automated data collection and processing in the 1960s gave rise to considerable discussions on its dangers in some European countries (in particular because of memories of the abuse of population and other public registers by Nazi occupiers in World War II), the US and the UK.[40] The common thread to the earlier development of laws around data protection of computer-based record keeping in Europe was the acknowledgement that automated data processing creates risks for individuals that existing legal frameworks, including confidentiality - privacy frameworks, could not adequately address.[41] The founding principle of data protection is that automated processing of personal data must be fair and the baseline assumption is that automated processing harms individuals unless the processing is done in compliance with the data management practices mandated by data protection law.[42]

---

[36] WHO (2021). *Ethics and governance of artificial intelligence for health.* P.11. Available at: https://www.who.int/publications/i/item/9789240029200

[37] General comment No. 16: Article 17 (Right to privacy) Thirty-second session (1988), Paragraph 10. Available at: https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=INT%2fCCPR%2fGEC%2f6624&Lang=en

[38] European Convention on Human Rights. Available at: https://www.echr.coe.int/documents/convention_eng.pdf

[39] Charter of Fundamental Rights of the European Union. (2000/C 364/01). Available at: https://www.europarl.europa.eu/charter/pdf/text_en.pdf

[40] Korff, D. & Georges, M. (2020, January 13).The Origins and Meaning of Data Protection. Available at: https://ssrn.com/abstract=3518386 or http://dx.doi.org/10.2139/ssrn.3518386

[41] The history of data protection law. Sep 20, 2018. Golden Data. Available at: https://medium.com/golden-data/data-protection-law-how-it-all-got-started-df9b82ef555e

[42] Ibid.

Protecting personal data or personally identifiable information (PII) entails establishing specific and unambiguous rules mandatory for any entity processing such data. Data protection and privacy laws have been in place in many countries around the world for more than 40 years but these laws are becoming increasingly important as people are now sharing more and more personal data, and governments and companies' data collection and use has skyrocketed. Today, hundreds of countries around the world have adopted general or sectoral data protection laws, and others are in the process of it.

1.3.2 Essential elements of a privacy and data protection law: EU GDPR

The European Union (EU) and its member states have had a long tradition of data privacy and security. The General Data Protection Regulation (GDPR) is considered a gold standard in this area and many countries, including India, are interested in replicating it. The critical provisions on privacy, data protection and digital rights in the GDPR that have also been quoted with approval by the landmark judgment of the Indian Supreme Court on the right to privacy [43] and advocated for inclusion in India's Digital Personal Bill 2022, are discussed below:

1.3.2.1 Privacy and data protection principles

The EU GDPR codifies (Article 5) eight privacy and data protection principles.[44] It lays down the necessary measures that any regulatory framework which seeks to effectively protect users' rights should include:

1) *Fairness and lawfulness:* Personal data should be collected, stored and processed fairly and lawfully. Information should be processed on a clear legal basis, for a lawful purpose and in a fair and transparent manner so that users are adequately informed about how their data will be collected, used, stored and by which individual/entity. These usually include the execution of a contract, compliance with a legal obligation and the user's consent. Consent should be defined as a dynamic, informed, voluntary and explicit request from the user, which should be capable of being withdrawn. In addition, governments and companies cannot deny users access to services for refusing to share more data than strictly necessary. Otherwise, consent is not considered to be freely given.
2) *Purpose limitation:* Personal data should be collected and processed for a specified and lawful purpose only. The purpose must be specific, explicit, and limited in time. Data should not be processed in any manner incompatible with the stated purpose.
3) *Data minimisation:* The use of collected personal data should be limited to what is adequate, relevant, and not excessive in relation to a specific and defined purpose.
4) *Accuracy:* The collected personal data should be accurate and up-to-date. Users have the right to erase, rectify, and correct their personal information.
5) *Retention or storage limitation:* Personal data processed for any purpose should not be kept for longer than is necessary.
6) *Users' rights:* Personal data should be processed in accordance with the users' rights to access, object, erasure, rectification, information, explanation, portability and not to be subject to automated decision-making. (For elaboration, see para 1.3.2.3 below)
7) *Integrity and confidentiality:* Personal data should be processed in a manner that ensures state-of-the-art security including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. (For elaboration, see para 1.3.2.2 below)

[43] *Justice K. S. Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1

[44] Privacy International. Data Protection Principles: A Guide for Policy Engagement on Data Protection. Available at: https://privacyinternational.org/sites/default/files/2018-09/Part%203%20-%20Data%20Protection%20Principles.pdf

8) *Adequacy:* Personal data should not be transferred to another country or territory unless that country or territory ensures an adequate level of protection for the rights and freedoms of users in relation to the processing of personal data.

The EU GDPR places the accountability on the data controller to demonstrate compliance with the privacy principles enumerated above (Article 5(2)).

1.3.2.2 Privacy by design

The EU GDPR codifies the concept of Privacy by design (PBD) (Article 25), The framework proactively embeds privacy directly into information technology, business practices, physical design, and networked infrastructures, assuring privacy to be the default.

The principle of PBD simply means 'data protection through technology design' – that data protection in data processing procedures is best sustained when integrated into the technology at the time of creation. By embedding PBD in both technology and organisational policy, privacy and data protection becomes part of the entity's culture and accountability framework rather than being a simple compliance element. There are seven foundational principles that constructs PBD to be a fundamental approach in systems development to mitigate data subjects' privacy concerns and achieve data protection compliance.[45]

1.3.2.3 Users' rights

The EU GDPR recognises eight users' rights aligned with the principles of privacy, transparency and accountability (Articles 12-23):

1) *Right to access* enables users to obtain confirmation from governments and companies as to whether personal data concerning them has been collected and is being processed.
2) *Right to object* enables users to say 'no' to the processing of their personal information, when they have neither given consent for such processing nor signed a contract. The right to object also applies to automated decision-making mechanisms including profiling, as users have the right not to be subjected to these techniques.
3) *Right to erasure* enables users to request the deletion of their personal data when they leave a service or application.
4) *Right to rectification* enables users to request modification of any inaccurate information about them.
5) *Right to information* ensures that users receive clear and understandable information from entities processing their personal data, including whether these entities have collected this information directly or received it through third parties. All the information provided to the user should be provided in concise, intelligible, and easily accessible form, using clear and plain language.
6) *Right to explanation* enables users to obtain information about the logical basis of any automatic personal data processing and the consequences of such processing. This right is crucial to bring accountability and transparency in the use of algorithms to make decisions that impact users' lives.
7) *Right not to be subject to automated decision making or profiling* The EU GDPR partly regulates AI systems, with rules on processing personal data and protecting data subjects against solely automated decision-making.

[45] Cavoukian, A. (2011). *Privacy By Design: The 7 Foundational Principles.* Available at: https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf

8) *Right to portability* enables users to move certain personal data they have provided from one platform to another offering similar services. To facilitate this process, interoperability between services needs to be encouraged as it is important for continuity of care.

Other provisions of EU GDPR which have also been advocated to be included in the Indian law on data protection include: the constitution of an independent regulatory authority; the undertaking of Privacy Impact Assessments and data breach notifications among others.

1.3.3 EU GDPR : Limits of data protection?

Although EU GDPR is appreciated for being progressive in terms of protecting users rights to privacy and data security, it has also been criticised by privacy groups[46] and activists for diluting privacy protections by including broad and vague exemptions. These include:

1. The EU GDPR provides a list of reasons that member states can rely on to restrict users rights and freedoms protected under the law (Article 23), such as "*national security*" or "*defence*". The GDPR also allows for restrictions of rights for broad and undefined "*other important objectives of general public interest of the Union or of a Member State*". Privacy advocates argue that given the impact of such restrictions on user's rights and freedoms, they should be clearly defined and limited in law, subjected to strict transparency and oversight criteria, and be necessary and proportionate measures in a democratic society.

2. The EU GDPR authorises processing personal data based on the legitimate interest of companies (one of the legal bases) without strict limitation (Article 6(1) (f)). The core of data protection is user's control and predictability in the use of their data. The legitimate interest provision goes against this principle. Under "*legitimate interest*" an organisation is authorised to collect and use personal information without having to notify the concerned users. One concern that has been posited is that if one does not know that an entity holds data on them, how could one exercise rights to access the data or the right to object? To enforce some accountability, the regulations require companies to balance their legitimate interest with fundamental rights. However, this does not amount to much protection as companies can conduct this assessment at their own discretion while keeping users in the dark. This overbroad exemption has given rise to different interpretations of "*legitimate interest*" and whether data processing for purely commercial interest could count as such.[47] This broad exemption given to companies has been one of the reasons that has galvanised large scale monetisation of data, including health data, the concerns around which are discussed in section 4 of this paper.

3. While as a general basis, EU GDPR requires organisations to collect sensitive personal data (such as health or genetic data) only with explicit informed consent of the users, it permits collection of sensitive data without consent for some specific objectives, including "*scientific or historical research purposes or statistical purposes*." This overly broad exception deprives users of control over their most intimate information, and becomes more problematic in the age of Big Data analyses. If not restricted, companies can gather and hoard sensitive information and make it difficult to conduct any oversight of how they use this data, as users will not be informed. This type of broad exemption should be avoided by restricting use of these data for research and statistical research conducted only in the public interest and under strict oversight.[48]

---

[46] Access Now (2018). Creating a Data Protection Framework: A Do's and Don'ts Guide for Lawmakers. Available at: https://www.accessnow.org/wp-content/uploads/2019/11/Data-Protection-Guide-for-Lawmakers-Access-Now.pdf
[47] Lexology (June 2022) European Commission criticises Dutch DPA's interpretation of legitimate interest. Available at: https://www.lexology.com/library/detail.aspx?g=a5116b17-9707-4825-93c9-438ef83913ba
[48] Access Now (2018). Creating a Data Protection Framework: A Do's and Don'ts Guide for Lawmakers. Available at: https://www.accessnow.org/wp-content/uploads/2019/11/Data-Protection-Guide-for-Lawmakers-Access-Now.pdf

1.4 Digital health and the right to health

The adoption of digital health technologies must align with the right to health under Article 12 of the International Covenant of Economic, Social and Cultural Rights (ICESCR). Applying the right to health framework to adoption of digital health technologies would entail decision-making for its implementation in a manner that ensures they are of reasonable quality, adequately available throughout the country, accessible in an equitable and non-discriminatory manner and acceptable to all. Table 1 illustrates some factors that must be considered in adoption of digital health, upon application of the right to health framework.[49]

Table 1: Applying the right to health framework for the implementation of digital health technologies	
Availability	Availability of digital infrastructure across the country, both in terms of hardware (e.g., computers, mobile phones, mobile phone towers, internet, and broadband accessibility) and software (e.g., applications)
Accessibility	Accessibility of technology (hardware, software, cost, language & user friendliness) for all but especially for vulnerable groups: people living in rural and remote areas, women, elderly, people with disabilities and mental health conditions, refugees and migrants.
	Provide digital literacy training for all users and health care workers
	Assess and address affordability barriers to digital hardware and software.
	Implement digital health with the objective to increase access to healthcare services for the most marginalised and assess progress towards this objective.
Acceptability	Protection of rights to consent, autonomy, confidentiality and privacy through legislation applicable to both state and non-state actors.
	Take into account user experience based on factors such as gender, sex, ethnicity and socio-economic differences.
Quality	Technology must be able to deliver on its clinical or public health purpose.
	Test or pilot prior to full-scale roll out and publish results.
	Train data handlers and other healthcare workers.

[49] United Nations Development Programme (2021). *Guidance on the rights-based and ethical use of digital technologies in HIV and health programmes.* https://www.undp.org/publications/guidance-rights-based-and-ethical-usedigital-technologies-hiv-and-health-programmes

Table 1: Applying the right to health framework for the implementation of digital health technologies	
	Set minimum quality standards and protocols for digital technologies.
	Conduct rigorous evaluation and assessment for evidence-based public health planning.
Equity and non-discrimination	Assess populations likely to be excluded due to unavailability and inaccessibility of the technologies due to digital divide.
	Ensure that effective non-digital options are available and accessible to all (whether unable or unwilling to use digital technologies) as an alternative to digital technologies.
	Account for the needs of vulnerable and marginalised groups, including women, children, racial and ethnic minorities, and migrants in design and adoption of digital tools.
	Assess likelihood of discrimination due to implicit biases within the technologies themselves, which perpetuate discrimination, such as artificial intelligence and machine learning.
	Carry out and publish human rights impact assessment before adoption of digital health technologies.
Participation	Ensure meaningful participation of end users and affected communities in the design, implementation and monitoring of digital technologies; as well as in development of laws and policies on digital health.
	Consider how digital health tools can be used by the community For example, within the HIV response, eHealth apps may be used by community members to monitor medication stockouts or to notify discriminatory treatment.[50]
	Develop mechanisms and institutions for democratic governance of health data to ensure that individuals and communities are enabled to determine that their data is used for public good.
Grievance redress	Ensure there are legal, regulatory and other accountability mechanisms to facilitate access to justice and redress for violations of human rights as a result of the development, implementation or use of digital technologies.

[50] Sun, N. et al. (2020). Human Rights and Digital Health Technologies. Health Hum Rights. Dec;22(2):21-32. PMID: 33390689; PMCID: PMC7762914.

1.4.1 Obligation of the government to respect, protect and fulfil the right to health

In the context of digital health, the obligation of the government to respect, protect and fulfil the right to health will at the minimum require it to ensure that the deployment of digital health technologies does not violate or undermine the fundamental rights to health, privacy and non-discrimination. Keeping that in mind, States must undertake human rights impact assessment of proposed digital technologies before their adoption. The obligation to respect, protect and fulfil the right to health also mandates a law to ensure protection of the rights to consent, autonomy, privacy and non-discrimination from state and non-state actors.

1.4.2 Obligations of private enterprise

Apart from governments, private companies also have human rights-related obligations including, at a minimum, the duty to respect human rights standards. In 2018, the OHCHR noted that its 'Guiding Principles on Business and Human Rights', published in 2011, imposes certain obligations on private companies and all entities that have access to personal data.[51] The obligations include the liability for violations of the right to privacy and the provision of effective remedies to redress violations.[52]

The guiding principles state that private companies "*must (a) avoid causing or contributing to adverse human rights impacts through their own activities, and address such impacts when they occur, and b) seek to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services by their business relationships, even if they have not contributed to those impacts.*"[53] In practice, private companies must develop and enact human rights policy commitments and conduct human rights due diligence, in keeping with privacy and data protection laws in their jurisdictions.

1.5 Right to benefit from scientific progress

In addition to the right to health framework, Article 15 of ICESCR, which enshrines the right to enjoy the benefits from scientific progress, is also relevant for digital health technologies. General Comment No. 25 on Article 15 [54] clarifies that countries have a duty to ensure the availability and accessibility of "*all the best available applications of scientific progress necessary to enjoy the highest attainable standard of heath*" [55] on a non-discriminatory basis, with a focus on the most marginalised.

As far as new and emerging technologies are concerned, the Committee clarifies that States should balance the benefits and risks of deploying them; they should be developed and used within an inclusive, rights-based framework, highlighting the principles of transparency, non-discrimination, accountability, and respect for human dignity. States should also introduce laws that impose an obligation for human rights due diligence on private and other non-state actors. States should also regulate the control and ownership of data collected through new technologies to prevent misuse and exploitation, as well as ensure informed consent and privacy.

1.6 International Health Regulations (IHR 2005)

The International Health Regulations (IHR) 2005 are contained in a legally binding agreement of 196 countries, including India, to build the capability to detect and report potential public health emergencies worldwide. One of the principles of the IHR is that "*the implementation of these Regulations shall be with full respect for the dignity, human rights and fundamental freedoms of*

[51] Report of the Office of the United Nations High Commissioner for Human Rights (2014). *The right to privacy in the digital age.* Available at: https://digitallibrary.un.org/record/777869?ln=en

[52] Office of the United Nations High Commissioner for Human Rights, *Guiding principles on business and human rights* (New York: United Nations, 2011). Available at: https://globalnaps.org/ungp/guiding-principle-13/

[53] Ibid.

[54] General comment No. 25 (2020) on article 15: science and economic, social and cultural rights. Available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G20/108/12/PDF/G2010812.pdf?OpenElement

[55] Ibid.

persons." (Article 3). It limits the ways in which personal data can be collected, stored and used for the purpose of disease surveillance. Article 45 requires that personal data be kept confidential and processed anonymously, as per national law. Where processing of personal data is considered essential, such circumstances must be grounded in law, and the data be handled fairly, lawfully, and proportionately.[56]

1.7 Ethical principles in the context of digital health technologies

In 2021, the United Nations Development Programme (UNDP) laid out key principles for the ethical use of digital health technologies, many of which are already established in public health and bioethics.[57] For example, the principles of 'do no harm' or non-malfeasance, and beneficence and well-being, imply that digital tools should not inflict any harm on people and should be deployed to maximise benefits while minimising harms. Similarly, the principle of transparency means that development, adoption and implementation of digital health technologies should be done in an open and discoverable manner that allows for public feedback, monitoring, and consultation. Other ethical principles include autonomy, informed consent, privacy, participation and inclusion, people centredness, non-discrimination and equity, and accountability.

The OHCHR's report**,** 'The right to privacy in the digital age'[58], analyses the implications of widespread use of AI including profiling, automated decision-making and machine-learning technologies on the enjoyment of the right to privacy and other associated rights. It recommends States to expressly recognize the need to protect and reinforce human rights as a central objective in the development, use and governance of AI; adopt and effectively enforce human rights through independent and impartial regulatory authorities, data privacy laws and other legislations to prevent and mitigate the multifaceted adverse human rights impacts linked to the use of AI; expressly ban AI applications that cannot be operated in compliance with international human rights law such as social scoring of individuals; require adequate explainability of all AI-supported decisions that can significantly affect human rights, particularly in the public sector; and ensure that public-private partnerships in the provision and use of AI technologies are transparent and subject to independent human rights oversight, and do not result in abdication of government accountability.

1.8 Health technology assessment of digital health technologies

Assessment and evaluation of technologies is part of both the international human rights framework as well as public health norms. The 2014 WHA resolution on health intervention and technology assessment in support of UHC urged States to adopt health technology assessment (HTA) as an important tool for evidence-based policy development and decision-making in health systems including decisions on resource allocation, service system designs and translation of policies into practice.[59] It also urged states to strengthen the link between HTA and regulation and management of medical devices.[60] HTA is a multidisciplinary systematic evaluation of healthcare technologies on

[56] WHO (2015). International Health Regulations. Available at: https://apps.who.int/iris/bitstream/handle/10665/246107/9789241580496-eng.pdf
[57] United Nations Development Programme (2021). *Guidance on the rights-based and ethical use of digital technologies in HIV and health programmes.* Available at: https://www.undp.org/publications/guidance-rights-based-and-ethical-usedigital-technologies-hiv-and-health-programmes
[58] Office of the United Nations High Commissioner for Human Rights (2021). The right to privacy in the digital age. Available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G21/249/21/PDF/G2124921.pdf?OpenElement
[59] World Health Assembly, 67. (2014). Health intervention and technology assessment in support of universal health coverage. Available at: https://apps.who.int/iris/handle/10665/162870
[60] WHO (2021) Institutionalizing Health Technology Assessment Mechanisms: A How To Guide. Available at: https://www.who.int/publications/i/item/9789240020665

parameters of safety assessment, clinical/medical effectiveness, cost-benefit analysis, social, ethical, and legal/regulatory.[61]

One strategy for preventing rights violations arising from digital health tools is the requirement for a robust system of HTA prior to their authorization. In 2021, UNDP recommended employing HTA frameworks to digital health technologies.[62] Applying HTAs to digital technologies provides an opportunity for governments to assess the ethical and human rights risks of these technologies, including equity considerations, and prevent the uptake of technologies that are of doubtful value for the health system.[63] For this, the traditional matrix of assessment will have to be expanded to accommodate digital health tools.[64] For instance, it should include strong focus on usability and human-centred design; requirement to co-design digital health tools with end users such as health care providers, systems administrators, patients, and affected communities, including effective mechanisms for subsequent feedback and iteration; obligation to conduct privacy and human rights impacts assessment prior to deployment. Governments and researchers are already actively considering and developing frameworks for HTA of digital health tools. For instance, the National Institute for Health and Care Excellence (NICE) in the UK has developed frameworks for assessment of digital health tools including AI.[65]

To summarise, while digital health has been recognised as potentially improving current challenges in availability and accessibility of health services, the pitfalls of digitalisation to have the opposite effect of its intended objective has also been established. International human rights law and practices expressly emphasise that the design, deployment and use of digital health technologies must be embedded in a rights-based framework and supported by robust laws, processes and systems that protect the rights to privacy and health.

2. DIGITAL HEALTH IN INDIA

India's foray into digital health began in the early 2000s. In 2006, the Indian government launched the National e-Governance Plan (NeGP), seeking to promote e-Governance initiatives across the country.[66] Around the same time, various public health information systems (HISs) were being set up under different national health programmes.[67] In 2011, the NeGP apex committee approved 'health' as one of its mission mode projects.

The National Health Policy 2017 further envisaged the creation of a digital health technology ecosystem, including an integrated national HIS, which *"serves the needs of all stakeholders and*

[61] O'Rourke B., Oortwijn W., Schuller T. the International Joint Task Group. The new definition of health technology assessment: a milestone in international collaboration. *Int J Technol Assess Health Care.* 2020;36(3):187–190. doi: 10.1017/S0266462320000215. [PubMed]

[62] United Nations Development Programme (2021). Guidance on the rights-based and ethical use of digital technologies in HIV and health programmes. UNDP (p. 10). Available at: https://www.undp.org/publications/guidance-rights-based-and-ethical-use-digital-technologies-hiv-and-health-programmes

[63] See https://www.paho.org/en/topics/health-technology-assessment

[64] Sun N. et al (2020). Human Rights and Digital Health Technologies. Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7762914/

[65] Office for Digital Health, NICE. Available at: https://www.nice.org.uk/about/what-we-do/digital-health/office-for-digital-health#evidence-standards-framework-update

[66] For more information on NeGP, see Ministry of Electronics and Information Technology, National e-Governance Plan. Available at: https://www.meity.gov.in/divisions/national-e-governance-plan..

[67] For an evaluation of various government HISs, see Faujdar et. al. (2019). *Public health information systems for primary health care in India: A situational analysis study*. J Family Med Prim Care 8(11), pp. 3640-3646. https://doi.org/10.4103%2Fjfmpc.jfmpc_808_19.

improves efficiency, transparency and citizens' experience."[68] In 2018, the Ministry of Health and Family Welfare released a draft Digital Information Security in Healthcare Act Bill (DISHA Bill), providing for the establishment of a National Digital Health Authority and HISs across the country.[69] Alongside, NITI Aayog proposed the idea of a National Health Stack, a shared digital infrastructure to facilitate collection of comprehensive healthcare data with linkages across public and private healthcare.[70] These initial efforts culminated in the National Digital Health Blueprint in 2019, which provides the layout for developing a digital health ecosystem, delivering a variety of digital health services such as telemedicine, hospital management systems, real-time public health surveillance and vaccination management.

On 15 August 2020, the Indian Prime Minister announced the National Digital Health Mission (NDHM).[71] In 2021, the NDHM was renamed the Ayushman Bharat Digital Mission (ABDM) and a nationwide rollout was announced.[72] The ABDM is an ambitious plan to build a digital health ecosystem that connects different stakeholders in the healthcare sector, both public and private. Alongside, the COVID-19 pandemic propelled the launch of several digital health applications, many of which are now integrated with the ABDM.

The stated objective of the ABDM is to create a digital health ecosystem that supports UHC by making the delivery of health services more efficient, accessible, equitable and affordable while maintaining good quality. That said, the proof of the pudding is in the eating. This section examines the legal and implementation issues encountered with the digitalisation of health in India and popular digital health applications developed and deployed by the central and state governments. The analysis is based on the frameworks of the international right to health and right to privacy, as well as ethical principles in the context of digital health technologies, as laid out in the preceding section.

2.1 Ayushman Bharat Digital Mission

A key aspect of the ABDM is to provide Ayushman Bharat Health Account (ABHA) IDs to every individual (or entity) and link the ABHA ID to the EHR of that individual (or entity).[73] EHRs are a longitudinal electronic version of patients' complete medical history (tests, diagnosis, treatment, prescriptions, etc.) that can be seamlessly and efficiently exchanged with healthcare providers, with the aim of facilitating health information exchange for patient care and secondary use, including research and healthcare planning. On 14 December 2020, the government approved the *National Digital Health Mission: Health Data Management Policy* (HDMP), to guide the development of the ABHA system, as well as facilitate the creation, storing, processing and sharing of individual EHRs.[74] In 2022, the Indian government approved the national roll-out of ABDM and allotted a budget of INR 16

[68] See, Clause 23, Government of India (2017). *National Health Policy 2017*. Ministry of Health and Family Welfare, Government of India (p. 25). https://nhsrcindia.org/sites/default/files/2021-07/National%20Health%20Policy%202017%20%28English%29%20.pdf.
[69] Government of India (2018). *Placing the draft of "Digital Information Security in Healthcare Act (DISHA)" in public domain for comments/views-reg*. F. No. Z-18015/23/2017-eGov. Ministry of Health and Family Welfare (eHealth Section). https://www.nhp.gov.in/NHPfiles/R_4179_1521627488625_0.pdf.
[70] Niti Aayog (2018). *National Health Stack: Strategy and Approach*. Government of India. https://old.abdm.gov.in/publications/NHS_Strategy_and_Approach.
[71] NDTV (Aug. 2020). PM Modi Announces National Digital Health Mission: "Health ID For Each Indian" [Video]. YouTube. https://www.youtube.com/watch?v=76L_Z28KFo.
[72] PMO's Office (2021). *PM to launch Ayushman Bharat Digital Mission on 27th September*. Press Information Bureau. https://pib.gov.in/PressReleasePage.aspx?PRID=1758248.
[73] NDTV (Aug. 2020). *PM Modi Announces National Digital Health Mission: "Health ID For Each Indian"* [Video]. YouTube. https://www.youtube.com/watch?v=76L_Z28KFo.
[74] Sharma, Neet Chandra (Dec. 2020). *Centre approves health data management HDMP of NDHM*. Livemint. https://www.livemint.com/news/india/centre-approves-health-data-management-HDMP-of-ndhm-11607962291863.html.

billion for the next five years.[75] For 2023-24, the government has committed INR 3.41 billion for the programme.[76]

The government has embarked on digitisation and deployed several digital health tools in the past few years without a legal framework and a weak policy in the form of the HDMP to govern the process. This despite there having been several instances of data breach and violation of the rights and civil liberties of persons in the last few years. For example, an April 2021 news report based on an RTI query revealed that the chief medical officer of Kulgam district in Jammu and Kashmir, was sharing *Aarogya Setu* users' data (without the users' knowledge and consent), with local police authorities.[77]

The Indian health sector has also suffered a spate of cyberattacks since the onset of the COVID-19 pandemic. On 23 November 2022, India's premier healthcare institution, the All-India Institute of Medical Sciences New Delhi, reported a suspected ransomware attack compromising the data of more than 30 million patients and crippling its services for almost two weeks.[78] About a week earlier, Safdarjung Hospital, another public hospital in New Delhi, also suffered a cyber-attack.[79] Around the same time, personal information of 150,000 patients who visited the Sree Saran Medical Hospital, a private hospital in Tamil Nadu between 2007 and 2011 were found on the dark web.[80] In May 2021, the Insurance Regulatory and Development Authority of India warned insurers against using leaked personal health records of COVID-19 patients to deny insurance coverage or block claims by policyholders.[81] In January 2021, a technology portal reported leaking of COVID-19 test results and personal information of thousands of patients, from the websites of multiple Indian government departments.[82] According to CloudSEK, a cyber intelligence company based in Bengaluru, India's health sector is the second-most targeted for cyberattacks in the world, accounting for 7.7% of all attacks on healthcare institutions in 2021 (only the US with 28% experiences more).[83] This raises serious questions as to whether the ABDM has adequate safeguards for its desired digital revolution in healthcare.

Successful implementation of a digital health records system also entails health system preparedness, i.e., an assessment of existing capacities for medical record documentation and health information exchange. Some studies, evaluating existing HISs in India, find several deficiencies on the poor quality of data being recorded, poor infrastructure support, the overburdened health workforce and social and cultural barriers.[84] The ABDM itself has run into several implementation hurdles. One report

---

[75] Press Trust of India (Feb. 2022). *Cabinet approves implementation of Ayushman Bharat Digital Mission with a budget of Rs.1,600 crore for five years*. PIB Delhi. https://pib.gov.in/PressReleasePage.aspx?PRID=1801322.
[76] Government of India. *Expenditure profile 2023-24*. https://www.indiabudget.gov.in/doc/eb/vol1.pdf.
[77] Bhatnagar, Gaurav Vivek (Apr. 2021). *Aarogya Setu Data Was Made Available to J&K Police in Kulgam, Reveals RTI*. The Wire. https://thewire.in/government/aarogya-setu-data-was-made-available-to-jk-police-in-kulgam-reveals-rti.
[78] Malhotra, Shefali (2023). *Cyberattacks hold up India's push for digitisation of health*. BMJ 2023, 380:p263. https://doi.org/10.1136/bmj.p263.
[79] Scroll Staff (2022). *Delhi's Safdarjung Hospital says it suffered a cyber attack in November*. Scroll.in. https://scroll.in/latest/1038970/delhis-safdarjung-hospital-says-it-suffered-cyber-attack-in-november
[80] IANS (2022). *Hackers now selling 150k patients' data of TN hospital on Dark Web: Report*. Business Standard. https://www.business-standard.com/article/current-affairs/hackers-now-selling-150k-patients-data-of-tn-hospital-on-dark-web-report-122120200647_1.html.
[81] Sengupta, Devina and Shukla, Saloni (May 2021). *Covid-19 patients' health data being sold on dark web*. Economic Times. https://telecom.economictimes.indiatimes.com/news/privacy-fears-around-patients-health-data-breach-amid-covid-surge/82600300.
[82] Sharma, Ax (Jan., 2021). *Indian government sites leaking patient COVID-19 test results*. Bleeping Computer. https://www.bleepingcomputer.com/news/security/indian-government-sites-leaking-patient-covid-19-test-results/.
[83] Mittal et al (2022). *Increased cyber attacks on the global healthcare sector*. CloudSEK. https://cloudsek.com/whitepapers-reports/increased-cyber-attacks-on-the-global-healthcare-sector.
[84] For example, see Deol, Taran (Apr. 2021). *Pharmacies were supposed to track Punjab's mild Covid cases, but this is why plan failed*. The Print. https://theprint.in/india/pharmacies-were-supposed-to-track-punjabs-mild-covid-cases-but-this-is-why-plan-failed/632358/; Sahay, S. et al (2018). *Grand challenges of public health: How can health*

highlights problems being faced by state governments in digitising patient records and setting up systems that work smoothly with others across the country, mainly due to a lack of expertise and capacity in procuring and implementing complex systems that will enable digitisation at the state and hospital level.[85]

The ABDM is also premised on the assumption of widespread internet connectivity throughout the country, as well as general comfort with using the internet. However, these assumptions may not hold true in most parts of the country. A 2022 study, published by the WHO, finds that in Europe, digital health tools tend to be used more widely in urban areas by younger populations and people with advanced education levels and high economic status, and less by minorities and those facing language barriers.[86] These findings may hold true for India as well.

According to the recently released survey results from the 71st round of the National Sample Survey Organization (NSSO), the proportion of Indian households in which at least one member had access to the internet was 16.1% in rural areas, 48.7% in urban areas and 26.7% in rural and urban areas combined.[87] Further, the latest National Family Health Survey (NFHS), covering 22 states and union territories, revealed that over 60% of women in 12 states and union territories have never used the internet.[88] Needless to say, this is far short of the near universal internet access envisaged by the ABDM. Age is also significantly associated with the digital divide. Across the world, younger people are more likely to use computers and the Internet than the older population.[89] The lack of exposure to and confidence with technology, coupled with issues of ageing and deteriorating senses and low literacy, are some of the drivers of low rates of digital literacy and technology usage among older people in rural areas, potentially exacerbating reticence to adopt digital health technologies.[90] There are also contours of caste that affect the digital divide and literacy landscape in India. Caste-based digital divide is rooted in the historical socioeconomic deprivation of disadvantaged caste groups. More than half of the caste-based digital gap is attributable to differences in educational attainment and income between the disadvantaged caste groups and others.[91] The digital gap between the Scheduled Castes and Scheduled Tribes (SC and ST) and others is enormous. For example, only 6% of SC and ST individuals had a computer at home compared to 20% of other individuals. Similarly, the

---

information systems support facing them? Health Policy and Technology, 7(1), pp. 2-3. https://doi.org/10.1016/j.hlpt.2018.01.009; Dehury, R.K and. Chatterjee, S.C (2018). *Assessment of health management information system for monitoring of maternal health in Jaleswar Block of Balasore District, Odisha, India*. Indian J Public Health, 62, pp. 261-263. Available at: https://doi.org/10.4103/ijph.ijph_203_17; Sharma et al (2016). *Quality of Health Management Information System for Maternal & Child Health Care in Haryana State, India*. PLoS ONE 11(2): e0148449, pp. 7-10. https://doi.org/10.1371/journal.pone.0148449.

[85] Jain, Anushka and Porecha, Maitri (Sept. 2022). *India's Rs 1,600-crore digital health ID mission is being squeezed at two ends*. The Ken. Available at: https://the-ken.com/story/indias-rs-1600-crore-digital-health-id-mission-is-being-squeezed-at-two-ends/?utm_source=IND&utm_medium=twt&utm_campaign=trd.

[86] WHO (2022). *Digital health not accessible by everyone equally, new study finds*. WHO. Available at: https://www.who.int/europe/news/item/21-12-2022-digital-health-not-accessible-by-everyone-equally-new-study-finds.

[87] Chandrasekhar, C.P (Jul. 2015). *The Internet in "Digital India"*. The Hindu. Available at: https://www.thehindu.com/opinion/columns/Chandrasekhar/economy-watch-column-by-cp-chandrasekhar-the-internet-in-digital-india/article7446778.ece.

[88] Press Trust of India (Dec. 2020). *Digital literacy remains a concern as most Indian women have never used the internet*. Economic Times. Available at: https://economictimes.indiatimes.com/magazines/panache/digital-literacy-remains-a-concern-as-most-indian-women-have-never-used-the-internet/articleshow/79736857.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst.

[89] Abbey, R. and Hyde, S. (2009). *No country for older people? Age and the digital divide*. Journal of Information, Communication and Ethics in Society, Vol. 7 No. 4, pp. 225-242. Available at: https://doi.org/10.1108/14779960911004480.

[90] Rasekaba, T.M et al (2022). *Exploring Telehealth Readiness in a Resource Limited Setting: Digital and Health Literacy among Older People in Rural India (DAHLIA)*. Geriatrics 2022, 7, 28. Available at: https://doi.org/10.3390/geriatrics7020028.

[91] Bhattacharya, Soham and Dam, Tinanjali (2020). *India's digital divide: Who faces it and how wide is it?* News Click. Available at: https://www.newsclick.in/india-digital-divide-who-faces-how-wide-it.

gap in computer literacy rate between other individuals and STs is 20 percentage points, which is the highest gap between the others and each of the disadvantaged caste groups.[92]

In this context it is important to highlight four limitations in the HDMP that make it a weak regulatory framework for implementing the ABDM and the ABHA system. These limitations fly in the face of the principles recognised as essential to the realisation of the rights to health and privacy.

2.1.1 Weak governance structure

The governance structure of ABDM is defined under Clause 6 of the HDMP. It is silent on the size, composition, selection process, tenure, powers, functions, terms of removal, financing and the accountability framework governing the ABDM. In contrast, the UK and Australian laws clearly lay out these details in respect of NHS-Digital and Australian Digital Health Agency, respectively.[93] The HDMP delegates the task of defining these parameters to the ABDM. In effect, the governance structure of ABDM will be laid out by ABDM itself. In practice, the National Health Authority (NHA), an executive body, governs the ABDM. It is not clear on what basis its members are selected, the procedure for selection and the terms of appointment. Such lack of clarity and transparency on the governance structure may open it up to partisanship, undue influence from the government and a lack of accountability to the general public.

2.1.2 Inadequate consent

Chapter III of the HDMP lays out a consent framework to govern the collecting, storing, processing and sharing of individual health data, with the objective that "*Data principals should at all times have control and decision-making power over the manner in which personal data associated with them is collected and processed further.*"[94] The HDMP rightly puts the autonomy of the data principal as its guiding principle, in relation to the collection, storage, processing and sharing of medical data. However, certain concerns remain.

First, the mandatory requirement of taking informed consent is limited to the collection and processing of personal data, and the same requirement is not explicitly extended to the creation of ABHA.[95] In September 2020, a government hospital in Chandigarh received an order stating that enrolling for the health ID was mandatory and urged the hospital to register its employees at the earliest.[96] While the NHA later clarified that the order was a "wrong circular", such cases create an atmosphere of confusion that may lead to the denial of services. Similarly, in January 2021, the Puducherry Directorate of School Education issued a circular directing all schools (public and private) to instruct parents to create Health IDs for all school-going children and their families.[97] More recently, multiple media reports have mentioned that citizens who have enrolled in the COVID-19 vaccination

[92] Rajam, V. et al (2021). *Explaining caste-based digital divide in India*. Telematics and Informatics, 65, 101719. https://doi.org/10.1016/j.tele.2021.101719.

[93] See, Schedule 18 of the UK *Health and Social Care Act 2012*; and the Australia *Public Governance, Performance and Accountability (Establishment of the Australian Digital Health Agency) Rule 2016*.

[94] See, Clause 8(a), *National Digital Health Mission: Health Data Management Policy 2020*.

[95] See, Clauses 9.1 and 10.1, *National Digital Health Mission: Health Data Management Policy 2020.*

[96] Rana, Chahat (2020). *Doctors in Chandigarh compelled to register for the voluntary National Health ID*. Caravan Magazine. Available at: https://caravanmagazine.in/health/doctors-in-chandigarh-compelled-to-register-for-the-voluntary-national-health-id .

[97] Mithun, M.K. (2021). *Privacy concerns loom as Union govt begins Health ID enrolment in Puducherry*. The New Minute. Available at: https://www.thenewsminute.com/article/privacy-concerns-loom-union-govt-begins-health-id-enrolment-puducherry-142987.

programme have had their Health IDs created without their consent or knowledge.[98,99] This is at odds with individual autonomy and choice, the guiding principle of the HDMP consent framework.

Second, the data fiduciary can secure one-time consent of the data principal for collecting and processing personal data for one or more broad purposes, as identified by the NDHM.[100] This is evident from the fact that the data fiduciary is required to collect fresh consent only in the event of any change in its privacy policy or in relation to any previously unidentified purpose.[101] It is also not clear whether informed consent is required for every instance of data anonymisation or de-identification. In 2021, the Karnataka High Court restrained the central government and the National Informatics Centre from sharing *Aarogya Setu* data without the informed consent of users.[102]

Third, the HDMP precludes the data principal from giving or refusing consent on specific lines. For example, the data principal will not be able to withhold consent to digitise specific information or even refuse consent to share specific digitised information, such as abortion, substance use/dependence, HIV/STI status, suicide attempt and other mental illnesses. Finally, the HDMP envisages an electronic consent manager system. However, low digital literacy levels may impede the ability of data principals to exercise consent in an informed and meaningful manner.[103]

2.1.3 Weak privacy and data security

The HDMP is based on PBD.[104] While this is a step in the right direction, the overarching concern of large-scale processing of health data in the absence of a data protection law remains. Without statutory guidelines for ensuring citizens' digital rights and the security of their data, effective data protection would be difficult to enforce. Even the procedures laid down in the HDMP do not contain adequate penalties for non-compliance as a deterrent. Additionally, concerns about surveillance that have been raised remain unanswered.[105]

The HDMP itself does not lay out a strong data protection regime. For example, it permits data processing, even when the data principal requests for erasure of data, till the purpose for which data was collected is no longer necessary.[106] The HDMP also allows the blocking or restriction of personal data in case of impairment of the legitimate interests of either the data principal or the health information provider.[107,108] These provisions may allow the health information provider or the data

---

[98] Mathew, Ashiln (2021); *Modi government issuing national health ID stealthily without informed consent*; The National Herald. Available at: https://www.nationalheraldindia.com/india/modi-government-issuing-national-health-id-stealthily-without-informed-consent.

[99] Dogra, Sarthak (2021); *Took Covid vaccine using Aadhaar? Your National Health ID has been created without your permission*; India Today. Available at: https://www.indiatoday.in/technology/features/story/took-covid-vaccine-using-aadhaar-your-national-health-id-has-been-created-without-your-permission-1806470-2021-05-24.

[100] For identified purposes, see National Digital Health Mission (2020). *Purposes for Collection and Use of Personal Data.* Notification No. T-21016/271/2020-eHealth/01. Available at: https://ndhm.gov.in/documents/hdmpolicy/notification/PurposeforCollectionandProcession.

[101] See, Clauses 10.1 and 10.2, *National Digital Health Mission: Health Data Management Policy 2020.*

[102] Express News Service (Jan. 2021). *Karnataka High Court restrains Centre, NIC from sharing Aarogya Setu data.* Indian Express. Available at: https://indianexpress.com/article/india/karataka-high-court-restrains-centre-nic-from-sharing-aarogya-setu-data-7161550/

[103] A 2017-18 NSO survey found that 18.4% of persons aged 15 and above were able to operate a computer, while 22.9% were able to use the internet. See, National Statistical Office (2020). *Household Social Consumption in Education in India, NSS 75th Round*. Available at: http://mospi.nic.in/sites/default/files/publication_reports/Report_585_75th_round_Education_final_1507_0.pdf.

[104] See, Clause 1, *National Digital Health Mission: Health Data Management Policy 2020.*

[105] Scroll Staff (September 6th, 2020). *New health data policy may be misused for surveillance: Chhattisgarh minister writes to Vardhan.* Scroll.in. Available at: https://scroll.in/latest/972361/new-health-data-policy-may-be-misused-for-surveillance-chhattisgarh-minister-writes-to-vardhan.

[106] See, Clause 14.1(b)(ii), *National Digital Health Mission: Health Data Management Policy 2020.*

[107] See, Clause 14.1(b)(ii), *Draft National Digital Health Mission: Health Data Management Policy 2020.*

[108] See, Clause 14.1(b)(ii), *National Digital Health Mission: Health Data Management Policy 2020.*

fiduciary to store and/or process the data principal's health data beyond the consented time-period and for longer than is necessary.

The HDMP does not envisage a strong accountability mechanism to enforce privacy. For example, in case of breach of security, only notifying the NDHM has been mandated, whereas notifying the data principal has not been made compulsory.[109] An established facet of a robust data protection framework is the reporting of any data breaches to the affected principals. Further, the carte blanche given for the processing and usage of anonymised personal data as 'non-personal' data ignores several attendant security hazards.[110] For example, several studies have indicated the increased threat of de-anonymisation, through both direct and indirect measures. When the scale of data expropriation by private entities contemplated by the draft report on the governance of non-personal data is considered, such concerns are only exacerbated.[111] The policy also provides the NDHM with discretionary power to specify acceptable purposes for collecting or processing health data, which may further contribute to excessive data collection.[112]

2.1.4 Weak enforcement

A grievance redress mechanism entails clear processes embedded in the rule of law, through which aggrieved parties can seek redress or challenge regulatory actions. The grievance redress process contained under chapter VII of the HDMP falls short on this count. While all data fiduciaries must appoint an internal grievance redress officer who has to resolve complaints within one month, the process for redress has been left to the discretion of the data fiduciary. The HDMP also does not provide the procedure for settlement of complaints before the NDHM Grievance Redress Officer (NDHM-GRO) or make any provision for appealing its decisions. In the absence of these procedures, data principals face the risk of arbitrary rejection of complaints.

The HDMP prescribes penalties for non-compliance. These include a ban from participating in the NDHE, and suspension or cancellation of digital IDs of health professionals and health facilities. While the HDMP envisages various degrees of possible contraventions, the penalties are limited to a ban, suspension or cancellation of the digital health ID. Being an executive policy, the HDMP cannot prescribe monetary penalties for violation of individual rights. This is yet another limitation of the policy route which lends to the argument that a non-statutory policy will prove to be illusory with respect to protection of rights. This may lead to situations where either minor violations go completely unpunished or a large number of penalties are disproportionate to the violation. Both scenarios will undermine implementation of the HDMP.

2.2 Digital health applications

Some of the major digital health applications whose development and deployment was propelled by the COVID-19 pandemic and have now been implemented across the country are discussed in this subsection. All these applications now form part of the ABDM ecosystem and are governed by the HDMP.

2.2.1 Aarogya Setu for digital contact tracing

In April 2020, the Government of India launched a contact-tracing app, *Aarogya Setu*, to assist public health officials in COVID-19 disease surveillance. It was developed by the National e-Governance

[109] See, Clause 33.2, *National Digital Health Mission: Health Data Management Policy 2020.*
[110] Internet Freedom Foundation. *Unconstitutional draft report on non-personal data ignores concerns about privacy and data monopolies*. Internet Freedom Foundation. Available at: https://internetfreedom.in/unconstitutional-draft-report-on-non-personal-data-ignores-concerns-about-privacy-and-data-monopolies/.
[111] Committee of Experts on Non-Personal Data Governance Framework (December 16th, 2020). *Draft Report by the Committee of Experts on Non-Personal Data Governance Framework: Version 2*. Mygov.in. Available at: https://static.mygov.in/rest/s3fs-public/mygov_160975438978977151.pdf.
[112] See, Clause 9.3, *National Digital Health Mission: Health Data Management Policy 2020.*

Division (NeGD) at the Ministry of Electronics and Information Technology (MeiTY), and was released in association with the Ministry of Health and Family Welfare (MoHFW). Today, the app is a data repository for individual health records created and maintained under the ABDM.[113] It is not being used for contact tracing anymore. In this section, we highlight six limitations in the design, deployment and implementation of *Aarogya Setu*. These limitations highlight the perils of implementing digital health technologies without adequate protections upholding the rights to health and privacy, as well as the resulting wastage of resources essential for implementing UHC in resource-limited settings such as India.

I. *Lack of transparency:* Digital contract tracing tools, at the time of deployment and even today, are considered novel untested tools with no conclusive evidence of their effectiveness. Ethical governance of digital health technologies demands that they be implemented in a transparent manner. However, the development and deployment of *Aarogya Setu* was opaque.[114] There was no formal oversight committee to govern the app and there was no public engagement in any form and at any stage of the deployment process. Even after implementation, there have been no independent audits of *Aarogya Setu*'s efficacy as a contact tracing app, other than press statements in which aggregate figures of detection of hotspots have been provided. These are advertorial rather than scientific claims not being open to peer review or scrutiny.

II. *Equity and inclusion*: In the initial days of COVID-19, central and state governments, as well as private organisations, mandated the installation of *Aarogya Setu* in order to access services, such as for airline travel. This was a significant disadvantage for those sections of the population that did not have access to smartphones. In May 2020, several technology rights and civil society organisations wrote to the Prime Minister's office protesting against the mandatory use of *Aarogya Setu.*[115]

III. *Excessive data collection:* The *Aarogya Setu* app collected proximity data using bluetooth and location data using the Global Positioning System (GPS). At the time, bluetooth data was considered a comparatively better tool for collecting data. This is because GPS location data, that allowed the government to track a user's precise location leaving them vulnerable to being directly identified, was considered unreasonably invasive of individual privacy. According to the MIT Technology Review, India, Bahrain, Norway and Qatar were the only four countries in the world that were collecting both Bluetooth and GPS location data through their contact tracing apps.[116] Apart from this, the app collected several data points including name, phone number, age, sex, profession and countries visited in the last 30 days. The level of personal information collected in this application was far beyond apps such as Singapore's TraceTogether and MIT's Private Kit: Safe Paths.[117]

---

[113] Ministry of Health and Family Welfare (2022). *Now generate your Ayushman Bharat Health Account (ABHA) number from your Aarogya Setu app.* Press Information Bureau. Available at: https://pib.gov.in/PressReleasePage.aspx?PRID=1797728.

[114] See, M. M., & Wang, C. J. (2020). *Ethics and governance for digital disease surveillance*. Science, 368(6494), 951-954 (p. 954). https://doi.org/10.1126/science.abb9045; Also see Ferretti, L. et al (2020). *Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing*. Science. 368(6491), p. 5. https://doi.org/10.1126/science.abb6936.

[115] The Wire Staff (2020). *Aarogya Setu Privacy Woes: Over 40 Organisations Push Back Against Mandatory Usage of COVID-19 App*. The Wire. Available at: https://thewire.in/rights/aarogya-setu-privacy-woes-letter.

[116] O'Neill, Patrick Howell et al. (2020). *A flood of coronavirus apps are tracking us. Now it's time to keep track of them.* MIT Technology Review. Available at: https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/.

[117] Deb, Sidharth (2020). *Privacy Prescriptions for technology interventions on COVID-19 in India.* IFF Working Paper No. 3/2020. Internet Freedom Foundation (p. 65). Available at: https://internetfreedom.in/a-comprehensive-look-at-covid-surveillance-and-privacy-in-india/.

IV. *Unreliable technology:* While Bluetooth data was considered comparatively less invasive, many security experts have argued that the technology itself is unreliable and inaccurate.[118] For instance, one expert has argued that environmental factors could make a Bluetooth device that is two metres away appear to another device as if it is 20 metres away, or vice versa. In addition, the technology can also suffer from path-loss variation, such as the Bluetooth signal colliding with a wall or getting absorbed by one's pants. Such a technology being used for contact tracing can lead to several false positives or false negatives, derailing containment measures by painting an inaccurate picture.

V. *Vague data sharing policy*: The privacy policy of *Aarogya Setu* has been criticised for being vague and non-specific as to how the data collected on the app would be utilised.[119] For one, it did not specify which government ministry, departments or officials will have access to the personal data of the users. While the primary purpose of the app was to inform users if they were at risk of COVID-19 exposure, the privacy policy also allowed the government to share personal data with '*other necessary and relevant persons*' for '*necessary medical and administrative interventions*'. Furthermore, this personal data could also be used for other purposes '*to comply with legal requirements.*' In May 2020, a month after *Aarogya Setu* was deployed, the government notified the Aarogya Setu Data Access and Knowledge Sharing Protocol. Notably, the privacy policy of the app did not refer to the 2020 protocol. In 2021, the Karnataka High Court, in *Anivar A. Arvind v Ministry of Home Affairs*, restrained the central government and the National Informatics Centre from sharing user data by applying the provisions of the 2020 protocol unless the informed consent of the users of *Aarogya Setu* app was taken.[120]

VI. Function *creep*: Central and state guidelines, whether on contact tracing or patient monitoring, uniformly insisted on the use of *Aarogya Setu*. In fact, not only was *Aarogya Setu* used for disease surveillance measures other than contact tracing, but also for purposes not related to disease surveillance at all. For example, an RTI query revealed that the chief medical officer of Kulgam district in Jammu and Kashmir, was sharing *Aarogya Setu* users' data (without the users' knowledge and consent), with local police authorities.[121] In another instance, a Delhi court mandated an accused to install *Aarogya Setu* as a condition for granting bail in the Northeast Delhi riots case.[122] In February 2022, the NHA announced the integration of *Aarogya Setu* with ABDM. The app was repurposed to become a repository for storing individual health records across health facilities.[123] These examples point towards 'mission creep' where individuals' personal data is being used for purposes beyond the purposes for which they were initially collected, thereby violating a recognised principle for processing personal data.

---

[118] Biddle, Sam (2020). *The Inventors of Bluetooth Say There Could Be Problems Using Their Tech for Coronavirus Contact Tracing*. The Intercept. Available at: https://theintercept.com/2020/05/05/coronavirus-bluetooth-contact-tracing/.

[119] Software Freedom Law Centre (2020). *Our Concerns With The Aarogya Setu App.* SFLC.IN. Available at: https://sflc.in/our-concerns-aarogya-setu-app; Deb, Sidharth (2020). *Privacy Prescriptions for technology interventions on COVID-19 in India.* IFF Working Paper No. 3/2020. Internet Freedom Foundation (pp. 66-67). Available at: https://internetfreedom.in/a-comprehensive-look-at-covid-surveillance-and-privacy-in-india/.

[120] *Anivar A. Aravind v Ministry of Home Affairs & Ors*. (2021). Karnataka High Court. WP no. 7483/2020. Available at: https://www.livelaw.in/pdf_upload/arogya-setu-388168.pdf .

[121] Bhatnagar, Gaurav Vivek (2021). *Aarogya Setu Data Was Made Available to J&K Police in Kulgam, Reveals RTI*. The Wire. Available at: https://thewire.in/government/aarogya-setu-data-was-made-available-to-jk-police-in-kulgam-reveals-rti.

[122] The Wire staff (2021). *Delhi Court Gives Umar Khalid Bail in Khajuri Khas Riots Case, Asks to Install Aarogya Setu*. The Wire. Available at: https://thewire.in/law/umar-khalid-delhi-court-khajuri-khas-riots-aarogya-setu.

[123] PIB Delhi (2022). *Now generate your Ayushman Bharat Health Account (ABHA) number from your Aarogya Setu App*. Press Information Bureau. Available at: https://pib.gov.in/PressReleasePage.aspx?PRID=1797728.

2.2.2 State and local mobile apps

A working paper, published by C-HELP in 2022, analyses 61 COVID-19 mobile apps, which were deployed by state governments and local authorities, based on four parameters, i.e., multiplicity of apps in every state, deployment process, integration of these apps with state public health protocols, and data privacy and security.[124] The paper finds inefficient use of limited public resources, lack of transparency and public engagement, mixed evidence on the integration of COVID-19 mobile apps with public health protocols, and weak data protection.

I. *Inefficient use of public resources*: States such as Karnataka, Kerala and Tamil Nadu deployed multiple mobile apps performing the same functions. The overlap in mobile apps was possibly due to the involvement of several government bodies in COVID-19 disease surveillance, including central and state governments, departments of health and family welfare, public health, and information technology, the police, district commissioners and municipal corporations. They all seem to have functioned in silos, with little to no interaction with each other at the time of developing and deploying COVID-19 mobile apps. Most of the apps were not led by public health departments of the state governments, and it was not clear how many of these apps were developed with epidemiologists at the helm.
II. *Lack of transparency and public engagement*: The processes followed by states and local authorities for the development and deployment of state and local mobile apps lacked transparency. There was a paucity of information available in the public domain on the various steps followed such as constituting oversight committees, selection of app developers and undertaking pilot studies. There were no public consultations and engagement preceding the launch of the apps or at any other stage.
III. *Mixed evidence on integration with public health protocols*: COVID-19 mobile apps are novel untested tools. Due to the lack of evidence on their effectiveness, these mobile apps cannot substitute but only supplement conventional contact tracing and quarantine monitoring measures. For this, they must be integrated with public health protocols on disease surveillance for contact tracing, quarantine and isolation. However, there is mixed evidence on the manner in which COVID-19 mobile apps for contact tracing and patient monitoring were integrated with public health protocols. Most public health protocols, with the exception of Karnataka and Surat, did not contain clear instructions on the use of COVID-19 mobile apps.
IV. *Weak data protection*: Privacy policies supporting state and local mobile apps afforded weak protection to individual privacy and data security. They did not meet internationally and domestically recognised standards for data processing, including purpose limitation, data minimisation, storage limitation, confidentiality and integrity, and transparency and accountability.

2.2.3 Telemedicine

The onset of COVID-19 in 2020 witnessed a manifold increase in the demand for remote healthcare. Subsequently, the Government of India introduced two verticals of e-Sanjeevani, its national telemedicine service launched in 2019: (a) the e-SanjeevaniOPD, a direct-to-care module to facilitate doctor-to-patient consultations using a smartphone, tablet or laptop, and (b) the eSanjeevaniAB-HWC to provide assisted teleconsultations at the Ayushman Bharat Health and Wellness Centres (AB-

[124] Malhotra, Shefali and Rai, Shivangi (2022). *To What Effect? COVID-19 Mobile Apps, Public Health and the Need for Sound Policy*. Centre for Health Equity, Law and Policy, Indian Law Society. Available at: https://www.c-help.org/wp-to-what-effect-covid-19-apps.

HWC).[125] In June 2022, the NHA announced the integration of eSanjeevani with ABDM.[126] Until December 2022, eSanjeevani had conducted a total of 80 million teleconsultations and issued 45000 ABHA IDs.[127] Alongside the national telemedicine service, the private health sector has also introduced telemedicine applications such as Practo and 1mg.

Telemedicine Practice Guidelines

In 2020, the *Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations 2002* was amended to permit telemedicine consultations by registered medical practitioners.[128] In the same year, the MoHFW issued the Telemedicine Practice Guidelines.[129] In 2022, these guidelines, now called the Guidelines for Practise of Telemedicine in India ("Telemedicine Guidelines"), were included in the draft National Medical Commission Registered Medical Practitioner (Professional Conduct) Regulations 2022.[130] They lay down the eligibility for practising telemedicine in India, the permissible modes and types of teleconsultations, and govern the doctor-patient relationship including informed consent, management protocols, quality and affordability of service and privacy and data security requirements. However, the protocols for informed consent and privacy and data security contain several deficiencies.

First, while on the one hand the Telemedicine Guidelines explicitly include informed consent as an essential element of teleconsultations, on the other they require that patient consent must be taken explicitly only when the registered medical practitioner (RMP) initiates the teleconsultation.[131] Consent is implied if a patient initiates a consultation. This is inadequate in the digital environment where the dynamics of a doctor-patient relationship are altered. Hence, consent must be taken only after informing the patient about the nature of teleconsultation, the technology used, potential for data abuse, the data protection measures undertaken by both the RMP and the technology platform, and the remedies available in case of any grievance.[132]

Other countries require health professionals to take informed consent of all patients irrespective of whether they initiated a teleconsultation or not. In Australia, the Federal Department of Health obligates health professionals to take informed consent of every patient.[133] In Japan, medical practitioners must enter into an agreement regarding telehealth with every patient, only after providing sufficient information to the patient.[134] In Singapore, the guidelines explicitly mention that patients must be free to make informed decisions and that healthcare providers should obtain informed consent before starting any service or intervention. It also requires that explicit consent be

[125] Business Standard (2021). *Health Ministry's eSanjeevani records 14 million consultations*. Available at: https://www.business-standard.com/article/economy-policy/health-ministry-s-esanjeevani-records-14-million-consultations-121101800978_1.html.
[126] Business Standard (2022). *eSanjeevani integrated with NHA's Ayushman Bharat Digital Mission*. Available at: https://www.business-standard.com/article/current-affairs/esanjeevani-integrated-with-nha-s-ayushman-bharat-digital-mission-122060300600_1.html.
[127] Ministry of Health and Family Welfare. (2022). *National telemedicine service of india - eSanjeevani achieves 8 crore teleconsultations* [Press Release]. Available at: https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1881185
[128] Clause 3.8, *Telemedicine Practice Guidelines* 2020.
[129] Ministry of Health and Family Welfare. (2021). *Telemedicine Regulations* [Press Release]. Available at: https://pib.gov.in/PressReleasePage.aspx?PRID=1740756.
[130] Regulations relating to Professional Conduct of Registered Medical Practitioners, F No. 12013/01/2022/Ethics (2022). Available at: https://www.nmc.org.in/MCIRest/open/getDocument?path=/Documents/Public/Portal/LatestNews/NMC%20RMP%20REGULATIONS%202022%20Draft%20Final%20YM.pdf.
[131] Section 3.4 *Telemedicine Practice Guidelines*, (2020).
[132] Lunt, Helen, et al (2019). *Electronic Informed Consent: The Need to Redesign the Consent Process for the Digital Age*. Internal Medicine Journal, vol. 49, no. 7, pp. 923–929. 10.1111/imj.14339.
[133] Medical Council of New Zealand. (2020). *Telehealth*. Available at: https://www.mcnz.org.nz/assets/standards/c1a69ec6b5/Statement-on-telehealth.pdf.
[134] DLA Piper Intelligence (2020). *Telehealth around the world: A Global Guide*. Available at: https://www.dlapiperintelligence.com/telehealth/countries/handbook.pdf?c=BR.

obtained from the patient for medical acts that would typically require explicit consent in the traditional health care setting such as video or audio recording of the sessions and use of data for research or educational purposes.[135] In Canada, the Ottawa provincial government requires that telehealth encounters be preceded by a communication to the patient on the risks and benefits of telemedicine, the choice to decline participation and alternatives available, how care will be documented, security, privacy and confidentiality of the information and the right to withdraw consent at any time.[136] In all of these instances, a clear emphasis has been given to reify the patient's autonomy, and prioritise the agency of the patient in health decision-making. Indeed, such a perspective augments health-seeking behaviour and improves engagement by and with the health system.

Second, the provisions on privacy and data security are deficient on several grounds.[137] First and foremost, India does not have a data protection law as of now. The law which exists – the *Information Technology Act 2000* – is outdated and inadequate. Moreover, this Act is not applicable to government services implying that it will not govern teleconsultations over the eSanjeevani platform. The Telemedicine Guidelines themselves will not govern all kinds of virtual interactions - teleconsultations by Ayurveda, Yoga and Naturopathy, Unani, Siddha and Homeopathy (AYUSH) practitioners, cross-border teleconsultations and the use of AI to assist RMPs. Further, the Telemedicine Guidelines do not impose any specific obligation on RMPs to ensure privacy and data security. For example, there is no explicit due diligence standard that RMPs must follow before they commit to using specific casual modes of communication for telemedicine such as Skype and WhatsApp. In contrast, the Ministry of Health in France has published a list of teleconsultation tools that meet the technical safety standards for the tools used. Similarly, the guidelines do not obligate RMPs to have a data breach action plan. The Australian Information Commissioner lays down a four-step data breach action plan for health service providers to contain and manage a data breach involving personal information.[138]

eSanjeevani Privacy Policy

The eSanjeevani privacy policy itself contains several deficiencies. For one, the policy does not specify the exact purposes for which the data that is collected on the app will be used, coining this in ambiguous terms. It states that the data will be stored on the app itself and will be used in anonymized form or as aggregated datasets only for the purpose of generating reports, statistical visualisations for purposes of research, academic, public health and health delivery.[139] That said, the policy prohibits disclosure or transfer of personal information to any third party except for information provided to persons who carry out intended medical and administrative interventions.[140] Yet, the integration of the app with ABDM and its use for creating ABHA IDs is an instance of function creep where the app is now being used for purposes other than teleconsultations.[141]

---

[135] Ministry of Health (2015). *National Telemedicine Guidelines for Singapore* (MH 25:22/1). Available at: https://www.moh.gov.sg/docs/librariesprovider5/licensing-terms-and-conditions/national-telemedicine-guidelines-for-singapore-(dated-30-jan-2015).pdf.

[136] National Initiative for Telehealth (2003). *Framework of Guidelines, Ottawa.* Available at: https://www.isfteh.org/files/work_groups/FrameworkofGuidelines2003eng.pdf.

[137] Clause 3.7.1.2 *Telemedicine Practice Guidelines*, (2020).

[138] Government of Australia (2020). *Data Breach Action Plan for Health Service Providers*. Available at: https://www.oaic.gov.au/privacy/guidance-and-advice/data-breach-action-plan-for-health-service-providers.

[139] eSanjeevani OPD (App.) (2020) *Clause 2 Privacy Policy*. Available at: https://esanjeevaniopd.in/PRIVACY_POLICY_eSanjeevaniOPD.pdf.

[140] eSanjeevani OPD (App.) (2020) *Clause 6 Privacy Policy*. Available at: https://esanjeevaniopd.in/PRIVACY_POLICY_eSanjeevaniOPD.pdf.

[141] Business Standard. (2022). *eSanjeevani integrated with NHA's Ayushman Bharat Digital Mission*. Available at: https://www.business-standard.com/article/current-affairs/esanjeevani-integrated-with-nha-s-ayushman-bharat-digital-mission-122060300600_1.html.

The policy also stipulates that personal information collected on the app will be retained for as long as a patient's account is in existence and in sync with the Telemedicine Guidelines.[142] It does not specify a time limit up to which EHRs of individuals may be stored. Moreover, personal information (other than EHRs) can be stored even after an account is deleted for academic, medical, public health or administrative interventions.[143]

Finally, the privacy policy does not specify the security features with which the app is equipped. It only states that personal information provided at the time of registration is encrypted before being uploaded to the cloud where it is stored in a secure encrypted server.[144] The app does not take any responsibility for any service provided through a third party. The privacy policy also does not mention the name and details of its internal grievance redress officer as stipulated under the HDMP.

2.2.4 CoWIN

With the development of COVID-19 vaccines, it became imperative to also develop a robust National Vaccination Strategy that could meet the needs of a large Indian population. To this end, the MoHFW launched the COVID-19 Vaccine Intelligence Network (CoWIN) in January 2021.[145]

With CoWIN, the objective was to achieve a comprehensive and staggered COVID-19 vaccine rollout in a number of ways. First, registration and booking of slots in advance could be a straightforward solution to prevent queues and crowding at vaccination centres, which could otherwise exacerbate the spread of infection. Second, CoWIN's design could disable automation or duplication by using CAPTCHA and OTP verification for every user. Third, it could prevent mixing of first and second dose vaccines and notify beneficiaries of their second-dose schedule. These objectives were incorporated into the design of the CoWIN website. CoWIN was subsequently also hosted on state-run mobile applications such as *Aarogya Setu*, UMANG and Digilocker.[146]

Based on an analysis of the design and processes of the CoWIN platform, key legal and implementation issues have arisen that are relevant to UHC.

I. *Equitable access*: Internet-based interventions in public policy are likely to face the issue of access, especially in remote and rural pockets of India. By bringing a universal immunisation drive online initially, CoWIN drew a social divide in who could access vaccines and who could not. Moreover, online registration was mandatory for people aged 18-44 years to avail of the vaccine. This placed the burden of immunisation on individuals, most of whom simply lacked the means to book appointments online for want of a smartphone or internet connection or could not understand the intricacies of CAPTCHA and OTP based verification.[147] On-site registration was made available by the central government a few months later, for those who

[142] eSanjeevani OPD (App.) (2020) *Clause 3 (a) Privacy Policy*. Available at: https://esanjeevaniopd.in/PRIVACY_POLICY_eSanjeevaniOPD.pdf.
[143] eSanjeevani OPD (App.) (2020) *Clause 2 Privacy Policy*. Available at: https://esanjeevaniopd.in/PRIVACY_POLICY_eSanjeevaniOPD.pdf.
[144] eSanjeevani OPD (App.) (2020) *Clause 5 Privacy Policy*. Available at: https://esanjeevaniopd.in/PRIVACY_POLICY_eSanjeevaniOPD.pdf.
[145] Special Correspondent (2021). *World's largest vaccination programme begins in India on January 16.* The Hindu. Available at: https://www.thehindu.com/news/national/coronavirus-worlds-largest-vaccination-programme-begins-in-india-on-january-16/article33582069.ece.
[146] UMANG, or Unified Mobile Application for New-age Governance, is a unified platform for users to access e-Gov services provided by central, state and local government bodies at one place. See: https://web.umang.gov.in/landing/aboutus. Digilocker is a secure cloud-based storage platform for users to store and access their authentic digital documents, and for other parties to verify user documents. See: https://www.digilocker.gov.in/.
[147] Lalwani, Vijayta ((2021). *A stark class divide is emerging in India's Covid-19 vaccination drive*, Scroll.in. Available at: https://scroll.in/article/989081/a-stark-class-divide-is-emerging-in-indias-covid-19-vaccination-drive.

could not register online following the Supreme Court's Essential Supplies Order.[148,149] Though walk-in vaccinations were eventually allowed, the MoHFW encouraged states and union territories to push for online registrations.[150]

II. *Technical errors*: When online registrations were mandatory, the process became harrowing and finding slots was next to impossible. Technical glitches, slow server speeds, OTP errors and simple unavailability of slots plagued the fraction of the population that could access CoWIN.[151] At the peak of the second wave of COVID-19, people started to develop codes and third party apps, or resort to bots, messaging groups, and middlemen to be informed of a free slot or for booking one for themselves and family.[152] The paid slots also varied in cost between states as well as for the two available vaccines, Covaxin and Covishield.[153]

III. *Data privacy*: By opening up the platform to millions of users, hospitals and third parties, CoWIN put a large repository of sensitive health data at risk of privacy breaches without an overarching remedial law to safeguard registered users. As stated earlier, privacy of health data is a recognised fundamental right, therefore tech-interventions like digitisation of vaccination records and linking them with one's identification documents require a legislative basis.[154] However, there was no data protection law in force in India when CoWIN was deployed.[155] Neither the privacy policy nor any CoWIN guidelines provide clarity on how data leaks will be avoided or addressed, especially when third parties are involved. In the absence of an overarching data law, CoWIN is a data repository prone to privacy breaches without any substantial procedural safeguards to fall back on.

IV. *Coercion and discrimination*: In many cases, registering via CoWIN generated the user's ABHA ID automatically and without express consent or knowledge.[156] In some instances, if one offered another identification document at hospitals for verification, they were asked to produce Aadhaar instead, consequently leading to a wider generation of ABHAs.[157] In *Siddharth Sharma v Union of India*, the Supreme Court clarified that the Aadhaar card could not be made mandatory and any of the other eight identity documents listed in the CoWIN Guidelines 2.0 could be produced.[158] Of the 23 crore Indians vaccinated against COVID-19, most used their Aadhaar to register and were allotted ABHAs without consent.[159]

---

[148] *In re: Distribution of Essential Supplies and Services During Pandemic.* Suo Moto WP (Civil) No. 3/2021 (Order dated 31 May 2021).

[149] Ministry of Health and Family Welfare. (2021). *On-site Registration/Facilitated Cohort Registration in addition to Online Appointment for 18-44 years age group now Enabled on CoWIN*. Available at: https://www.pib.gov.in/PressReleasePage.aspx?PRID=1721225.

[150] Ministry of Health and Family Welfare. (2021). *India administers more than 20 lakh Covid-19 doses in a single day*. Available at: https://pib.gov.in/PressReleseDetailm.aspx?PRID=1703641.

[151] Alluri, Aparna (2021). *India's Covid vaccine shortage: The desperate wait gets longer*. BBC. Available at: https://www.bbc.com/news/world-asia-india-56912977.

[152] Sathe, Gopal (2021). *CoWIN Vaccine Registration Alert Bots in India Lead to Spike in Users for Telegram.* NDTV Gadgets 360. Available at: https://gadgets360.com/apps/features/cowin-telegram-india-bots-covid-19-vaccine-coronavirus-applications-new-registrations-2442147.

[153] Kumar, Parimal (2021). *Covishield At 780, Covaxin At 1,410: Maximum Price For Private Hospitals.* NDTV. Available at: https://www.ndtv.com/india-news/covishield-at-780-covaxin-at-1-410-sputnik-v-at-1-145-maximum-price-that-can-be-charged-for-vaccines-by-private-hospitals-2459353.

[154] *Justice K. S. Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1.

[155] ETech Staff (2022). *Government withdraws Data Protection Bill, 2021*. The Economic Times. Available at: https://economictimes.indiatimes.com/tech/technology/government-to-withdraw-data-protection-bill-2021/articleshow/93326169.cms.

[156] Dogra, Sarthak (2021). *Took Covid vaccine using Aadhaar? Your National Health ID has been created without your permission.* India Today. Available at: https://www.indiatoday.in/technology/features/story/took-covid-vaccine-using-aadhaar-your-national-health-id-has-been-created-without-your-permission-1806470-2021-05-24.

[157] Rana, Chahat (2021). *COVID-19 vaccine beneficiaries were assigned unique health IDs without their consent*. The Caravan. Available at: https://caravanmagazine.in/health/covid-19-vaccine-beneficiaries-were-assigned-unique-health-ids-without-their-consent.

[158] *Siddharth Sharma v Union of India*. (2021). Supreme Court of India. WP (Civil) no. 656/2021.

[159] Qureshi, Mehab (2021). *Govt Created Health IDs Without Consent, Say Vaccinated Indians*. The Quint. Available at: https://www.thequint.com/tech-and-auto/govt-created-ABHA-without-consent-say-vaccinated-indians#read-more

There were several instances where COVID-19 vaccination was made a prerequisite for accessing essential services. Villages in Karnataka, Madhya Pradesh and Jammu & Kashmir had observed a "no vaccine, no ration" policy for months before it was officially halted.[160] The Assam government had threatened to withhold salaries of government employees who were not vaccinated.[161] District administrations had issued orders to cut salaries of unvaccinated government employees in Satna, Ujjain, Rewa and Datia in Madhya Pradesh, and Firozabad and Bareilly in Uttar Pradesh.[162] States like Odisha, Uttar Pradesh, Madhya Pradesh, Meghalaya, Mizoram and Manipur passed orders restraining people from running their business or practising their professions without getting vaccinated.[163] West Bengal restricted entry to public parks without a vaccination certificate.[164] Rajasthan has passed a similar order for all public places while Kerala restricted entry to shopping malls.[165] In May 2022, the

[160] Trivedi, Vivek (2021). N*o Vaccine–No Ration: Panchayat Diktat in Madhya Pradesh Improves Inoculation*. News18. Available at: https://www.news18.com/news/india/no-vaccine-no-ration-panchayat-diktat-in-madhya-pradesh-improves-inoculation-3834737.html; Dainik Bhaskar Team (2021). *If There Is No Vaccine Then There Is No Ration, If People Reach Then The Vaccine Is Over (Translated)*. Dainik Bhaskar. Available at: https://www.bhaskar.com/local/mp/bhopal/raisen/news/if-there-is-no-vaccine-then-there-is-no-ration-if-people-reach-then-the-vaccine-is-over-128632300.html; Menasinakai, Sangamesh (2021). *'No vaccine, no ration' slogan in Gadag village*. Times of India Available at:. https://timesofindia.indiatimes.com/city/bengaluru/no-vaccine-no-ration-slogan-in-gadag-village/articleshow/83275311.cms; Ganai, Naseer (2021). *J&K Govt Revokes Controversial 'No Vaccine, No Ration' Order After Outrage; Check Details.* Outlook. Available at: https://www.outlookindia.com/website/story/india-news-j-check-details/379432.

[161] Choudhury, Ratnadip (2021). *Assam Government Employees' Body Criticises No Vaccine, No Salary Plan.* NDTV. Available at: https://www.ndtv.com/india-news/assam-government-employees-body-criticises-no-vaccine-no-salary-plan-2472664.

[162] Livemint Team (2021). *No vaccine, no salary: Madhya Pradesh district collector tells govt staff*. Livemint. Available at: https://www.livemint.com/news/india/no-vaccine-no-salary-madhya-pradesh-district-collector-tells-govt-staff-11624430361629.html; Afridi, Shahroz (2021). *Bhopal: Salary cuts to rewards like TV, fridge for getting jab.* The Free Press Journal. Available at: https://www.freepressjournal.in/bhopal/bhopal-salary-cuts-to-rewards-like-tv-fridge-for-getting-jab; Business Today Team (2021). COVID-19: *No salary without vaccination for govt employees in this UP district*. Business Today. Available at: https://www.businesstoday.in/latest/economy-politics/story/covid-19-no-salary-without-vaccination-for-govt-employees-in-this-up-district-298170-2021-06-02; Singh, Kanwardeep (2021). *No salary to government employees without vaccination certificate: Lakhimpur Kheri DM's diktat*. Times of India. Available at:https://timesofindia.indiatimes.com/city/bareilly/no-salary-to-govt-employees-without-vaccination-certificate-kheri-dms-diktat/articleshow/83522631.cms.

[163] Mohanty, Debabrata (2021). *Odisha district makes vaccination compulsory for traders*. Hindustan Times. Available at: https://www.hindustantimes.com/india-news/odisha-district-makes-vaccination-compulsory-for-traders-101623925757266.html; Times Now Team (2021). *Uttar Pradesh: Vaccination is mandatory for businessmen who are 45 years and above or else would not be allowed to open their shops*. The Economic Times. Available at: https://economictimes.indiatimes.com/news/india/uttar-pradesh-vaccination-is-mandatory-for-businessmen-who-are-45-years-and-above-or-else-would-not-be-allowed-to-open-their-shops/videoshow/83253586.cms?from=mdr; Times Now Team (2021). *Bhopal: Shop owners, employees rush to get vaccinated ahead of reopening of markets*. Times of India. Available at: https://timesofindia.indiatimes.com/videos/toi-original/bhopal-shop-owners-employees-rush-to-get-vaccinated-ahead-of-reopening-of-markets/videoshow/83380014.cms; Thapliyal, Nupur (2021). *Breaking: 'Forced Vaccination Violates Fundamental Right': Meghalaya High Court.* Livelaw. Available at: https://www.livelaw.in/top-stories/forced-vaccination-violates-fundamental-right-rules-meghalaya-high-court-176216; Parashar, Utpal (2021). *Curbs on unvaccinated violate rights: Gauhati HC*. Hindustan Times. Available at: https://www.hindustantimes.com/india-news/curbs-on-unvaccinated-violate-rights-gauhati-hc-101625424546869.html ; HT Correspondent (2021). *Denying people livelihood by linking jobs to jabs is illegal: Manipur HC*. Available at: https://www.hindustantimes.com/india-news/denying-people-livelihood-by-linking-jobs-to-jabs-is-illegal-manipur-hc-101626372848700.html.

[164] Rajaram, Prema (2021). *West Bengal: Covid vaccination certificates mandatory to enter parks but not hotels, malls.* India Today. Available at: https://www.indiatoday.in/india/west-bengal/story/covid-vaccination-certificates-mandatory-parks-1815273-2021-06-15.

[165] FP Staff (2021). *Rajasthan eases curbs, but makes at least one COVID shot mandatory to enter public places from 28 June*. Firstpost. Available at: https://www.firstpost.com/india/rajasthan-eases-curbs-but-makes-at-least-one-covid-shot-mandatory-to-enter-public-places-from-28-june-9756151.html; Express News Team (2021). *Kerala makes Covid negative papers or vaccination must to enter shopping malls*. The Indian Express. Available at: https://www.newindianexpress.com/states/kerala/2021/apr/16/kerala-makes-covid-negative-papers-or-vaccination-must-to-enter-shopping-malls-2290511.html.

Supreme Court in *Jacob Puliyel v Union of India* restricted public and private from issuing COVID-19 vaccination mandates.[166]

V. *Grievance redress*: The HDMP creates a grievance redress mechanism that requires a data principal to first internally resolve their complaint with a data fiduciary, in this case CoWIN. However, the CoWIN grievance redress system is complicated and very limited in scope.[167] One is expected to log into the CoWIN portal via OTP and file only one of eight kinds of complaints, all related to corrections and adding information. There is no avenue for a data breach complaint to be filed, as the online form has only drop-down menus. CoWIN's privacy policy is also unhelpful in this regard.[168] Beyond the CoWIN framework, the HDMP gives one an option to escalate to the ABDM's grievance redressal officer, but does not provide the procedure for the same. This could lead to arbitrary dismissal of complaints or unlawful proceedings.

VI. *Function creep*: One cornerstone of the constitutional doctrine of proportionality is that an intervening measure should be designated for a specific purpose.[169] For a technology like CoWIN, this implies having a purpose limitation to the kind of uses the collected personal data can be put to. The platform defied this principle in a number of ways since its conception by introducing new use cases and features that involved health data initially collected for the simple and specific purpose of vaccination. Firstly, CoWIN was used as a medium to roll out ABHAs without the consent or knowledge of its users. Secondly, CoWIN was integrated with Aarogya Setu to allow users to access their vaccination certificates.[170] Thirdly, hundreds of third parties were allowed to integrate with the platform via public and restricted Application Programming Interface (API), making the vast CoWIN database vulnerable to misuse.[171] Fourthly, an API was introduced in later stages which allowed employers and service providers to access the vaccination status of an individual without their knowledge or consent. Fifthly, the central government rolled out a facial recognition system with CoWIN.

The ABDM is the Government of India's ambitious programme to digitise healthcare in India with the stated objective of supporting UHC in India. The various digital health applications, such as the ones discussed above, are already or will form part of the programme. While there are many purported benefits of doing so, it also fundamentally alters the way Indians interact with the healthcare system and poses serious risk to their rights to privacy, confidentiality, access and good quality of health services. Hence, it is imperative that the implementation of the ABDM and various digital health applications be supported by adequate laws, policies, processes and systems in place. To this extent, active and sustained stakeholder engagement will provide a strong feedback loop to aid in the development of the ABDM and digital health applications. The analysis presented in this section reveals that the current policy framework governing ABDM and the deployment of digital health tools have not conformed with international and domestic framework governing the rights to privacy and health. In fact, in many instances of deployment both of these rights have been violated.

The next section discusses implications of AI, big data analytics and data monetisation by private entities in the health sector.

---

[166] *Jacob Puliyel v Union of India.* Supreme Court of India. WP. (Civil) no. 607/2021.

[167] C*itizen Grievance Resolution: User Manual* (Version 3.0) (2022). Ministry of Health and Family Welfare. Available at: https://prod-cdn.preprod.co-vin.in/assets/pdf/Grievance_Guidelines.pdf.

[168] *Privacy Policy*. CoWIN Website. Available at: https://www.cowin.gov.in/privacy-policyhttps://www.cowin.gov.in/privacy-policy.

[169] *Modern Dental College & Research Centre v State of Madhya Pradesh & Ors.* (2010) SC Civil Appeal no. 4060/2009.

[170] Tech Desk (2021). *Aarogya Setu gets CoWIN app integration: How to access Covid-19 vaccination information.* The Indian Express. Available at: https://indianexpress.com/article/technology/techook/cowin-aarogya-setu-covid-19-vaccination-registration-info-7183975/.

[171] An API, or Application Programming Interface, is a channel of communication between two applications or software programmes, enabling one to retrieve information from the other. In this context, CoWIN APIs allow any third-party application to access information on registered CoWIN users.

3 ARTIFICIAL INTELLIGENCE IN THE HEALTH SECTOR

In recent years, there has been growing interest in the application of AI in healthcare. The WHO defines AI as, "*the ability of algorithms encoded in technology to learn from data so that they can perform automated tasks without every step in the process having to be programmed explicitly by a human.*"[172] In 2019, the United Nations Secretary General recognised the important role of safely deployed technologies, including AI, in achieving sustainable development goals.[173]

AI covers a range of different techniques such as machine learning, where big data is used to effectively train algorithms to recognise patterns or perform behaviours using tight feedback loops that improve accuracy. It is created using a two-step process: a) creation of intelligence to solve a problem by getting the algorithms to learn from historical data (big data) and b) application of this learning to new situations to generate insights. Essentially AI systems are prediction engines that take information one has to generate information one does not; but they do not give rationales for their recommendations. The use of AI has increased exponentially in the healthcare industry for predictive analysis to prevent future harms, manage patient risk trajectories, and recommend personalised interventions.

Proponents of AI believe it has the potential to revolutionise health. Its various applications have been used in clinical practice, biomedical research, public health and health administration. Some examples include medical image quantification, automated analysis of genetic data, disease prediction, medical robotics, telemedicine and virtual doctors.

In 2018, Niti Aayog was tasked to develop a national programme on research and development in artificial intelligence.[174] Subsequently, it published a discussion paper, 'National Strategy for Artificial Intelligence #AIForAll' that demonstrates how AI can be successfully applied to five sectors - healthcare, agriculture, education, smart cities and infrastructure, and smart mobility and transportation to benefit the country's population.[175] Building further on the national strategy, it published broad ethics principles for the design, development and deployment of AI applications in 2021.[176] The report identified safety and reliability, equality, inclusivity, privacy and security, transparency, accountability and protection and reinforcement of positive human values, as core principles.

However, AI in healthcare comes with its own challenges. In 2020, the United Nations Secretary General emphasised the need for designing and implementing AI in an accountable manner, in order for it to have any significant impact on access and delivery of health services. In particular, the Secretary General noted the significant risk that AI and big data pose to patients' right to privacy regarding sensitive health data and other personal information.[177]

---

[172] See, WHO (2021). Ethics and Governance of Artificial Intelligence for Health: WHO Guidance. World Health Organisation (p. xi). Available at: https://www.who.int/publications/i/item/9789240029200.
[173] See, United Nations (2019). Report of the Secretary-General on SDG Progress 2019: Special Edition (p. ii). United Nations, New York. Available at: https://sustainabledevelopment.un.org/content/documents/24978Report_of_the_SG_on_SDG_Progress_2019.pdf.
[174] Jaitley, Arun (2018). Budget 2018-19: Speech of Arun Jaitley, Minister of Finance. Available at: https://www.indiabudget.gov.in/budget2018-2019/ub2018-19/bs/bs.pdf.
[175] NITI Aayog (2018). National Strategy for Artificial Intelligence: #AIForAll. NITI Aayog. Available at: https://indiaai.gov.in/research-reports/national-strategy-for-artificial-intelligence.
[176] Niti Aayog (2021). *Responsible AI #AIForAll: Approach Document for India Part 1 - Principles for Responsible AI*. NITI Aayog. Available at: https://www.niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf.
[177] United Nation Secretary General (Feb. - Mar. 2020). Question of the realisation of economic, social and cultural rights in all countries: the role of new technologies for the realisation of economic, social and cultural rights: Report of the Secretary General. A/HRC/43/29. https://www.ohchr.org/en/documents/reports/ahrc4329-report-role-new-technologies-realization-economic-social-and-cultural.

In 2021, the UN Office of the High Commissioner for Human Rights (OHCHR highlighted, "the undeniable and steadily growing impacts of AI technologies on the exercise of the right to privacy and other human rights, both for better and for worse. It has pointed to worrying developments, including a sprawling ecosystem of largely non-transparent personal data collection and exchanges that underlies parts of the AI systems that are widely used." It urged governments to adopt legislative and regulatory frameworks that adequately prevent and mitigate the multifaceted adverse human rights impacts linked to the use of AI by public and private actors.[178]

This section traverses some key ethical and human rights concerns associated with AI in health.

3.1 Not all AI algorithms are successful or reliable

While AI tools are easily accessible to the general public, there is often limited information on how AI algorithms have been developed and validated, while their reliability and clinical efficacy is not always demonstrated. During the pandemic several AI tools were developed to diagnose infected patients without much success. Unrealistic expectations led to the deployment of AI tools that were not equipped to achieve the desired goals. For example, an analysis of hundreds of medical AI tools for diagnosing and predicting COVID-19 risks, published by the MIT Technology Review, found that none made a real difference and some were potentially harmful.[179]

In another instance, a 2020 review of nine different studies that evaluated six mobile apps for skin cancer detection, published in the British Medical Journal, demonstrated their lack of efficiency and high risk for bias. The authors concluded that "*current algorithm-based smartphone apps cannot be relied on to detect all cases of melanoma or other skin cancers*" and that current regulatory processes for algorithm-based apps does not provide adequate protection to the public.[180]

3.2 Risk of diagnostic error

AI-guided clinical solutions in healthcare may be associated with failures that could potentially result in safety concerns for the end-users of healthcare services. It may lead to false negatives in the form of missed diagnoses of life-threatening diseases, unnecessary treatments due to false positives, unsuitable interventions due to imprecise diagnosis, or incorrect prioritisation of interventions in the emergency department. The scalability of AI solutions can dramatically increase negative effects of seemingly small error rates.

For instance, a 2018 study on company DeepMind's deep learning model[181] trained on a large dataset for automated diagnosis of retinal diseases, published in Nature, found that the AI system was confused when applied to images obtained from a machine that is different from the one used for data acquisition at the AI training stage, with the diagnosis error increasing from 5.5% to a staggering 46%.[182] Another study, published in the AMA Journal of Ethics in 2019, analysed AI predictions for

---

[178] United Nations Secretary General (Feb. 2021). Secretary-General Guterres calls for a global reset, "to recover better, guided by human rights". Speech to the Human Rights Council. Available at: https://www.ohchr.org/en/statements-and-speeches/2021/02/secretary-general-guterres-calls-global-reset-recover-better-guided?LangID=E&NewsID=26769.

[179] Heaven, Will Douglas (2021). Hundreds of AI tools have been built to catch covid. None of them helped. MIT Technology Review. Available at: https://www.technologyreview.com/2021/07/30/1030329/machine-learning-ai-failed-covid-hospital-diagnosis-pandemic/.

[180] Freeman, K. et al (2020). Algorithm based smartphone apps to assess risk of skin cancer in adults: systematic review of diagnostic accuracy studies. BMJ (Clinical research ed.), 368, m127. https://doi.org/10.1136/bmj.m127.

[181] Deep learning model is a computer model that learns to perform classification tasks directly from images, text, or sound.

[182] De Fauw, J. et al (2018). Clinically applicable deep learning for diagnosis and referral in retinal disease. Nat Med 24, pp. 1342–1350. https://doi.org/10.1038/s41591-018-0107-6.

intensive care unit mortality and found that the use of AI resulted in a higher error rate for female patients than for males.[183]

3.3 Black box AI – lack of transparency and explainability

The decision-making processes of many AI systems are opaque, which makes it challenging to meaningfully scrutinise an AI system and can be an obstacle for effective accountability in cases where AI systems cause harm. Such AI solutions are often described as 'black-box AI'. For instance, an AI algorithm developed by Google for breast cancer screening received considerable attention for its promising performance. However, the work was also criticised for lack of transparency. One critique noted that "the absence of sufficiently documented methods and computer code underlying the study effectively undermines its scientific value. This shortcoming limits the evidence required for others to prospectively validate and clinically implement such technologies."[184]

3.4 Challenges of assigning liability

AI algorithms can assist doctors with diagnosis, as they can process large volumes of clinical literature, images, health records, and test results. However if doctors are relying on diagnostic or treatment suggestions made by AI, would it amount to medical advice?[185] Another ethical dilemma relates to more widespread use of AI that may lead to replacing certain tasks altogether, such as the ability to read an X-ray. Such dependence on AI could adversely impact independent human judgment and handicap clinicians and healthcare workers if the technology makes mistakes or fails.[186] Several ethical and liability questions arise in relation to this new technology frontier, all of which have a bearing on rights-based approaches to health, and indeed, to equitable UHC. Should AI be regulated? If so, how - as a human being or as a medical device? Is it possible to assign a personhood and affix liabilities on AI? If not, who should be held responsible for mistakes made and harm caused? And, therefore, at the very least should not these tools be designed for use under supervision of a doctor, instead of being used to replace them? Irrespective of the answers to these questions, since AI algorithms are opaque and its recommendations unexplainable, relying on them and consequences of doing so will continue to be a problem.

It is imperative to address medical malpractice and product liability that arise with the use of "black-box" algorithms because users cannot provide a logical explanation of how the algorithm arrived at its given output. A 2022 study shows malpractice claims involving robot-assisted surgical procedures in the US have increased more than 250% in the past 7 years compared to the seven years prior.[187]

3.5 Risk of bias and discrimination exacerbating inequality

Medical care is plagued by inequalities and inequities on grounds of sex, gender, age, race, ethnicity, income, education and geography which is codified in the data sets. AI algorithms trained on these data sets will further entrench discrimination against already marginalised communities. Additionally, algorithm developers may unknowingly introduce biases to AI algorithms or train the algorithms using incomplete datasets. In a 2021 report, the Cloud Security Alliance (CSA), a non-profit organisation that

---

[183] Chen, I., Szolovits, P., Ghassemi, M., Can AI Help Reduce Disparities in General Medical and Mental Health Care? AMA J Ethics. 2019; 21(2):E167-179. 10.1001/amajethics.2019.167.

[184] Haibe-Kains, B. (2020). *Transparency and reproducibility in artificial intelligence*. Nature, 586, E14–E16 (2020). Available at: https://doi.org/10.1038/s41586-020-2766-y.

[185] Matthan, R. and Pipraiya, P. (2023). Artificial Intelligence and Healthcare. in Parsheera, S (ed.) *Private and Controversial: When Public Health and Privacy Meet in India*. Harper Collins. pp. 287-309.

[186] Academy of Medical Royal Colleges (Jan. 2019). *Artificial Intelligence in Healthcare*. Academy of Royal Medical Colleges (p. 24-25). Available at: https://www.aomrc.org.uk/wp-content/uploads/2019/01/Artificial_intelligence_in_healthcare_0119.pdf.

[187] De Ravin, E. et al (2022). Medical malpractice in robotic surgery: a Westlaw database analysis. Journal of Robotic Surgery, pp. 1-6. Available at: https://pubmed.ncbi.nlm.nih.gov/35554817/.

promotes best practices for securing cloud computing, suggested that the rule of thumb should be to assume that AI algorithms contain bias and work to identify and mitigate those biases.[188]

Algorithms to predict costs have been used by private insurers, for-profit hospitals, academic groups and governmental agencies. For example, Optum, the tech focused arm of United Health Group, a US-based health and wellness company, deployed an algorithm in US hospitals that predicted severity of illness and resources needed, depending upon past spending data.[189] The algorithm did not take into consideration other societal factors in making these predictions, resulting in race-based discrimination in the care provided to patients in hospitals. Less money is spent on black patients with the same level of need as white patients, causing the algorithm to conclude that black patients were less sick. This meant less resource allocation for a group which already suffers racial discrimination, hence compounding the discrimination further, with disastrous outcomes for health.

In another instance, a 2020 Canadian study, presented at the Pacific Symposium on Biocomputing, evaluated the extent to which state-of-the-art deep learning algorithms detecting abnormalities in chest X-rays are biased.[190] The study found extensive patterns of bias against underrepresented sections of society such as young females, Hispanic patients and people with Medicaid insurance.

The above examples illustrate the limitations of poorly defined problem-solving applications for algorithms, and underscores the need for such assessments to be complimented by and situated within broader socio-economic and historical contexts, a knowledge that only humans have.[191] The question of whether AI will replace human workers assumes that AI and humans have the same qualities and abilities. AI-based machines may be fast, and in the best-case scenario, more accurate, and consistently rational, but they are not intuitive, emotional, or culturally sensitive, and have a problem of inference.[192] It is these unique abilities – to imagine, anticipate, feel, and judge changing situations, which allows humans to shift from short-term to long-term concerns and therefore makes them more effective. These abilities do not require a steady flow of externally provided data to work as is the case with AI.[193]

3.6 Risk to privacy

Use of AI can cause privacy intrusion in several ways: through the use of identifiable images; due to inadequate de-identification of location data in data sets resulting in individual patients being identified (for instance, when making heat maps for diseases), and the use of AI in individualised precision medicine requiring the constant surveillance of patients, and the collection of planned and unplanned data (such as in assisted living for elderly patients where AI has been noted to be constantly listening in).[194] In another instance, a study on Apple's ResearchKit (discussed above), which used the iPhone for Parkinson's disease clinical research revealed that the AI was capturing

[188] Health IT Analytics Editorial Staff (2022). *Arguing the Pros and Cons of Artificial Intelligence in Healthcare*. Health IT Analytics. Available at https://healthitanalytics.com/news/arguing-the-pros-and-cons-of-artificial-intelligence-in-healthcare

[189] Ledford, Heidi (2019). Millions of black people affected by racial bias in health-care algorithms. Nature. Available at: https://www.nature.com/articles/d41586-019-03228-6.

[190] Seyyed-Kalantri, Leleh (2021). *CheXclusion: Fairness gaps in deep chest X-ray classifiers.* Pacific Symposium on Biocomputing 26:232-243 (2021). Available at: https://psb.stanford.edu/psb-online/proceedings/psb21/seyyed-kalantari.pdf.

[191] Cremer, David De and Kasparov, Garry (2021). *AI should augment human intelligence, not replace it*. Harvard Business Review. Available at: https://hbr.org/2021/03/ai-should-augment-human-intelligence-not-replace-it.

[192] Ibid.

[193] Ibid.

[194] Matthan, R. and Pipraiya, P. (2023). *Artificial Intelligence and Healthcare*. in Parsheera, S. (Ed.). *Private and Controversial: When Public Health and Privacy Meet in India. .* Harper Collins. pp. 181-199.

individualised digital fingerprints of the subjects outside research parameters, making it possible to identify them.[195]

In 2021, the WHO released its guidance on the ethics and governance of the design, development and deployment of AI in the health sector.[196] It highlighted six key principles: protecting human autonomy, promoting human well-being, safety and public interest, ensuring transparency, explainability and intelligibility, fostering responsibility and accountability, ensuring inclusiveness and equity, and promoting responsive and sustainable AI. The European Parliament and the European Council have been deliberating a law governing AI applications in the EU since 2021.[197] The law proposes to take a risk-based approach, classifying different AI applications as minimal risk, limited risk, high risk and unacceptable risk, allowing free use of minimal risk AI and prohibiting AI applications with unacceptable risk. Under this law, many AI applications in healthcare, such as robot-assisted surgery and digital medical devices, will be classified as high-risk. In October 2022, the US White House Office of Science and Technology Policy also proposed an AI Bill of Rights.[198] Today, about 60 countries have national AI strategies and many are contemplating laws to regulate the use of AI.[199]

4 BIG DATA ANALYTICS AND HEALTH DATA MONETISATION IN THE PRIVATE SECTOR

This section examines emerging technologies that will play a part in health delivery and therefore have significant implications for UHC. It highlights the role of monetization of health data in the private sector, using big data analytics and AI and the impact on rights to informed consent, autonomy, privacy, data protection, equity and non-discrimination and the broader impact on health. The increasing inroad of Big Tech in digital health is focused on, and the risks posed by anti-competitive practices of digital monopolies on the State's capacity to protect rights and fulfil its obligation of right to health and UHC. The disruptive changes brought about by digital health in the insurance and pharmaceutical sector and the legal ethical questions that they leave in their wake, which spans a range of rights having a bearing on achievement of right to health and UHC, are also discussed.

Data monetization refers to the process of using data to obtain quantifiable economic benefits.[200] Organisations can monetize their data by providing data access to third parties, commonly referred to as direct monetization, or by using analytics to derive insights from data to improve internal processes, products, and services, known as indirect monetization.[201] Data monetisation will be driven by the increasing magnitude of big data sets, increasing awareness of commercial benefits of data monetisation, emerging technology trends such as Business Intelligence and Analytics (BI&A), cloud computing, blockchain, Internet of Things (IoT), social networks and post-COVID-19 pandemic business approaches and strategies.[202]

---

[195] Ibid.
[196] WHO (2021). Ethics and Governance of Artificial Intelligence for Health. World Health Organisation. Available at: https://www.who.int/publications/i/item/9789240029200.
[197] European Commission (2021). Proposal for laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts. Available at: https://artificialintelligenceact.eu/the-act/.
[198] The White House (2022). Blueprint for an AI Bill of Rights. White House. Available at: https://www.whitehouse.gov/ostp/ai-bill-of-rights/.
[199] Firth-Butterfield, Kay et al (2022). *Understanding the US 'AI Bill of Rights' - and how can it help keep AI accountable.* World Economic Forum. Available at: https://www.weforum.org/agenda/2022/10/understanding-the-ai-bill-of-rights-protection/.
[200] Mixson, E. (2021, August 1). *Measuring and Maximising Data ROI: A Quick Guide to Data Monetisation.* AI Data & Analytics Network. Available at: https://www.aidataanalytics.network/data-monetization/articles/a-quick-guide-to-data-monetization
[201] Ibid.
[202] Ofulue, J. & Benyoucef, M. (2002). Data monetization: insights from a technology-enabled literature review and research agenda. *Manag Rev Q.* Available at: https://doi.org/10.1007/s11301-022-00309-1.

A BIG TECH, DIGITAL HEALTH AND DATA MONETISATION

4.1 Big Tech's strident march in digital health

As the digital healthcare market has grown, major tech companies such as *Google, Microsoft, Amazon and Apple* are intensifying their efforts to enter the healthcare sector and have begun to focus their strategy on particular areas of the ecosystem. From cloud services to wearable monitors, "*big tech has invested in deals worth a cumulative USD 6.8 billion since the start of 2020.*"[203] They are backing or acquiring innovative start-ups, developing new products, and strategically partnering to build their positions in the industry. Gathering, leveraging, and monetizing data is a guiding force in Big Tech's healthcare activity. These corporations are all competing to be the cloud platform of choice for healthcare providers, software developers, and life sciences organisations.[204]

In 2020, the COVID-19 pandemic accelerated this trend by precipitating the emergence of new initiatives. Examples include Google's subsidiary Verily offering COVID-19 testing and tracing, Google and Apple cooperating on mobile operating systems for COVID-19 contact tracing, and Amazon offering COVID-19-specific Amazon Web Services (AWS) solutions for hospitals and research institutes.[205]

Big Tech is also entering the insurance and pharmaceutical sectors, particularly in clinical trials and research. In fact, lines are blurring between different actors and sectors – digital medical device players, insurance companies, pharmaceutical and Big Tech companies are all undertaking mergers and acquisitions or buying data sets from one another. For instance, CVS Pharmacy, currently the largest pharmacy chain in the United States, acquired Aetna, a health insurance company; and is combining its pharmaceutical data with Aetna's pool of insurance data.[206] This is causing transformation and disruption with significant implications.

Google **-** Over the last decade, Google's role *"has evolved from that of a peripheral IT service provider to healthcare incumbents to that of an increasingly present and central actor in the industry."*[207] This entry pathway has led to Google not only entering several of the sector's niches, but also becoming an "*essential partner to infrastructural projects for government agencies and state-controlled institutions, dominating the industry for diagnostics, electronic health records, enhancement of current devices and treatments, and development of new devices and treatments in healthcare*."[208]

- Alphabet-Google partnered with United Kingdom's National Health Service (NHS) for data sharing and developing AI-powered healthcare services to provide predictive healthcare
- Acquired the wearable giant Fitbit opening new doors for tracking of health data.
- Acquired Senosis Health, an app using smartphone sensors as monitoring devices.

[203] Thomason, J. (2021). Big tech, big data and the new world of digital health. *Global Health Journal*. Available at: https://doi.org/10.1016/j.glohj.2021.11.003.
[204] CBINSIGHTS (2022). The Big Tech in Health Care Report. Available at: https://www.cbinsights.com/research/report/famga-big-tech-healthcare/.
[205] Ozalp, H. et al. (2022). "Digital Colonization" of Highly Regulated Industries: An Analysis of Big Tech Platforms' Entry into Health Care and Education. *California Management Review*, *64*(4), 78–107.
[206] Lin, M. *Everything you need to know about the CVS Aetna Deal.* Finance Processes. Toptal. Available at: https://www.toptal.com/finance/mergers-and-acquisitions/cvs-aetna.
[207] Ozalp, H. et al. (2022). "Digital Colonization" of Highly Regulated Industries: An Analysis of Big Tech Platforms' Entry into Health Care and Education. *California Management Review*, *64*(4), 78–107.
[208] Ibid.

- Google's health venture Claico uses the genetic data and other related information of individuals to address the problems relating to ageing.

Microsoft - Microsoft's role evolved from being an IT service provider to becoming an increasingly essential partner to many healthcare institutions through its cloud platform, Azure, and data analytics.[209]

- Healthcare NExT utilises AI and Azure to connect data from different sources to accelerate innovation by combining research and health product development.
- Research collaboration with UPMC named Project EmpowerMD, to reduce the burden of note making for doctors by listening and learning from what they say.
- Its cloud based health bot platform allows organisations in the healthcare industries to create AI powered health bots and virtual assistants
- Microsoft Genomics provides care providers as well as clinical researchers with fast-paced cloud-powered genomic processing services.

Apple - Apple maintains a dominance in the mobile and wearable devices market and leverages these devices to collect individual-level data for diagnosis. It is transforming wearables like the Apple watch into patient health hubs and clinical research tools.[210]

- It has developed kits to facilitate the development of health care applications for the iPhone and Apple Watch. The Healthcare Kit and the Research Kit allow developers to create apps for medical research and recruit participants for studies/clinical trials.
- Partnerships with universities like Duke University School of Medicine and Stanford University Hospital to allow chronically ill patients to remotely track and manage their symptoms.[211]
- The Apple Watch allows users to track different health related activities such as sleeping habits, blood oxygen levels, heart rhythms, period tracking etc.[212]
- Apple Health Records lets individuals store their medical data on their phones.

Amazon - Amazon is relying on its cloud arm Amazon Web Services (AWS) and voice tech expertise to offer services to hospitals. It is using acquisitions and large-scale partnerships to launch new

[209] Insider Intelligence (2023, January 24). *Big Tech in Healthcare: Here's who wins and loses as Alphabet, Amazon, Apple and Microsoft target niche sectors of healthcare.* Insider Intelligence. Available at: https://www.insiderintelligence.com/insights/big-tech-in-healthcare-report/.
[210] Ibid.
[211] ACC News Story (2019, March 16). *Apple Heart Study Identifies AFib in small group of Apple Watch Wearers.* American College of Cardiology. Available at: https://www.acc.org/latest-in-cardioSalogy/articles/2019/03/08/15/32/sat-9am-apple-heart-study-acc-2019.
[212] Muoi, D. (2019, June 28). *Apple Health Records now available to all US providers with compatible EHRs,* Mobi Health News. Available at: https://www.mobihealthnews.com/news/north-america/apple-health-records-now-available-all-us-providers-compatible-ehrs.

healthcare projects[213] to transform the pharmacy, the medical supply chain, health insurance, and care delivery.[214]

- The Amazon Transcribe Medical transcribes doctor-patient interactions and plugs the text straight into the medical record.
- It acquired the online pharmacy start-up Pillpack to enter into online retail of medicines.
- The virtual voice assistant, Amazon Echo is offering assistance in identifying diseases by asking health questions and analysing the answers given.

4.2 Big Tech in Digital health - Impact on rights

4.2.1 Violation of informed consent, autonomy, privacy and transparency

To capture data, Big Tech firms engage in two types of activities simultaneously: using their own hardware or software to build their own data sets; and/or forming partnerships with state or private actors for access to existing data.[215] Collection of personal data for profiling and targeted advertisements, without informed consent, and lack of transparency in deals is one of the biggest issues that has cropped up with the emergence of Big Tech conglomerates in health. Several instances of this invasive data capture have been documented.

In 2019, Google's controversial Project Nightingale with Ascension, the second largest healthcare provider in the USA, triggered a federal inquiry. It reportedly collected people's medical data in order to create AI powered software, without the patient or their doctor's consent.[216]

In 2017, the UK's data protection watchdog ruled that a deal to share 1.6 million NHS patient records with the Google-owned artificial intelligence company DeepMind "*failed to comply with data protection law.*"[217]

Google's acquisition of Fitbit is under investigation by the US Justice Department on consent, privacy and competition concerns. Through acquisition of Fitbit, Google could combine all users' health and fitness data along with data collected through other Google services, without any legal basis to do so, and without users' consent.[218]

---

[213] Insider Intelligence (2023, January 24). *Big Tech in Healthcare: Here's who wins and loses as Alphabet, Amazon, Apple and Microsoft target niche sectors of healthcare.* Insider Intelligence. Available at: https://www.insiderintelligence.com/insights/big-tech-in-healthcare-report/.

[214] Ibid.

[215] Ozalp, H. et al. (2022). "Digital Colonization" of Highly Regulated Industries: An Analysis of Big Tech Platforms' Entry into Health Care and Education. *California Management Review*, *64*(4), 78–107.

[216] Copeland, R. & Needleman, S.E. (2019, November 12). *Google's 'Project Nightingale' Triggers Federal Inquiry.* The Wall Street Journal. Available at: https://www.wsj.com/articles/behind-googles-project-nightingale-a-health-data-gold-mine-of-50-million-patients-11573571867.

[217] Revell, T. (2017, July 3). *Google DeepMind's NHS Data Deal 'failed to comply' with law*. NewScientist. Available at: https://www.newscientist.com/article/2139395-google-deepminds-nhs-data-deal-failed-to-comply-with-law/

[218] Robertson, A. (2019, December 11). T*he Justice Department will reportedly investigate Google's Fitbit acquisition.* The Verge. Available at:https://www.theverge.com/2019/12/10/21009870/justice-department-doj-google-fitbit-acquisition-antitrust-review-data-privacy-ftc

Amazon's pill pack (online pharmacy start-up) made unsolicited phone calls to other chemists and pharmacies requesting them to transfer the prescriptions that they had to Amazon. This often occurred without the customer's knowledge or consent.[219]

In spite of the GDPR being fully in force, by the end of 2019, Big Tech advertising by Google, Amazon, Facebook and Oracle were found to have been dropping cookies "*and collecting clearly sensitive data from website users of a number of popular health websites in the UK, allowing them to track and serve targeted ads without their explicit consent.*"[220] A study found that regulators in EU countries had imposed fines on Big Tech companies for infringing GDPR adding up to 114 million euros.[221]

4.2.2 "Digital colonialism": Big Tech and anti-competitive practices

There has been rising global scrutiny of tech giants for allegedly abusing their market position using chunks of user data. The US Congress spent over 15 months investigating the monopolist dominance of the country's largest tech firms and proposed measures to rein them in.[222] Its report found that:

a) "*Over the past decade, the digital economy has become highly concentrated and prone to monopolization*", and that "*just a decade into the future, 30% of the world's gross economic output may lie with these firms, and just a handful of others*."[223] The report states that this has and will continue to negatively impact competition and innovation.
b) Further, in the absence of adequate privacy guardrails, "*the persistent collection and misuse of consumer data is an indicator of market power online*."[224] The report stated that "*courts and enforcers have found the dominant platforms to repeatedly violate laws and court orders. This pattern of behaviour raises questions about whether these firms view themselves as above the law*."[225]
c) Finally, the market power of the monopolies risks undermining both political and economic liberties. "*the growth in the platforms' market power has coincided with an increase in their influence over the policy making process. Through a combination of direct lobbying and funding think tanks and academics, the dominant platforms have expanded their sphere of influence, further shaping how they are governed and regulated.*"[226]

In this context, the flurry of acquisitions and push of Big Tech into the healthcare sector have raised serious concerns related to autonomy, privacy, institutional and regulatory capacities of the states, as well as impact on competition and innovation in the health sector. Researchers have studied the

[219] Farr, C. (2019, August 6). *Amazon's Pillpack is battling with CVS and Walgreens over getting patient prescriptions.* CNBC. Available at: https://www.cnbc.com/2019/08/06/amazons-pillpack-expansion-faces-resistance-from-cvs-and-walgreens.html
[220] Editor's Choice (2020, February 24). *The rise of big tech monetising healthcare data.* Information Age. Available at: https://www.information-age.com/rise-big-tech-monetising-healthcare-data-15457/
[221] Ibid.
[222] Kang, C. & McCabe, D. (2020, October 6). *House Lawmakers Condemn Big Tech's 'Monopoly Power' and Urge Their Breakups.* The New York Times. Available at: https://www.nytimes.com/2020/10/06/technology/congress-big-tech-monopoly-power.html
[223] Subcommittee on Antitrust, Commercial and Administrative Law of the Committee on the judiciary of the House of Representatives, United States of America. (2022). *Investigation of Competition in the digital markets, Part 1*. US Government Publishing Office. Available at: https://www.govinfo.gov/content/pkg/CPRT-117HPRT47832/pdf/CPRT-117HPRT47832.pdf
[224] Ibid. Pages 10, 11, 12 of the House Judiciary Report
[225] Ibid.
[226] Ibid.

pattern of entry of Big Tech in the digital health industry and have termed the process and outcome as "digital colonialism". They describe the process as below:[227]

a) Big Tech Companies typically begin as "*suppliers of data-infrastructure services to hospitals/state.*" As service providers such as hospitals lack capabilities in data management, they contract out these activities to Big Tech, aiming to reduce cost and improve services.
b) In the second phase, Big Tech leverages their existing relationships and their data analysis capabilities to get access to the data already held by service providers. These firms combine this indirectly acquired data (termed indirect data capture) with their own direct data capture activities (e.g., through IoT and wearables such as Apple Watch). This is described as an essential component of Big Tech firms' entry into the health sector.
c) Big Tech firms combine the data they capture directly and indirectly, to provide superior data-driven insights, which can add significant value to service providers.
d) In the final stage, Big Tech firms design and commercialise new products and services, where they may end up competing with their former clients over time.

Elaborating on the impact, the researchers conclude that "*Big Tech companies change the power dynamics in these industries over time by commoditizing original service providers, turning them into mere complementors while Big Tech firms control the data and become unique providers of critical, data-driven value.*"[228] The WHO Report on Ethics and Governance of Artificial Intelligence for Health, acknowledges the challenges of tech monopolies in health and states that "*monopoly power can concentrate decision-making in the hands of a few individuals and companies, which can act as gatekeepers of certain products and services and reduce competition, which could eventually translate into higher prices for goods and services, less consumer protection or less innovation*."[229]

4.3 Public-private partnerships with Big Tech in digital health in India

Given the push to operationalise ABDM and expectation from states to digitise quickly, coupled with the present lack of data infrastructure and analytics capacity, several states are entering into agreements with Big Tech firms such as Google, Amazon and Microsoft, to build health data infrastructure, data analytics and generating insights from data. Such public-private partnerships (PPPs) in the absence of a comprehensive data protection law combined with the lack of institutional as well as data governance capacity at the state level, raise serious questions regarding privacy of personal health data, risks of monetisation of personal health data, and propping up tech monopolies in the digital health space through capture of data as well as operations.

4.3.1 The Kerala government's agreement with Sprinkler

The Kerala government collected data using a mobile app developed by Sprinkler, a US based tech firm and also shared data of 1.75 lakh people under quarantine with the firm, to help plan the response to the COVID-19 pandemic.[230]

There was severe criticism of the deal over privacy and national security issues, with a petition being filed in the High Court challenging the deal. The High Court issued an interim order requiring the data to be anonymised and only shared with the informed consent of all concerned individuals, to protect

[227] Ozalp, H., et al. (2022). "Digital Colonization" of Highly Regulated Industries: An Analysis of Big Tech Platforms' Entry into Health Care and Education. *California Management Review*, *64*(4), 78–107. Available at: https://doi.org/10.1177/00081256221094307
[228] Ibid.
[229] World Health Organisation (2021). *Ethics & Governance of Artificial Intelligence for Health*. Available at: https://www.who.int/publications/i/item/9789240029200
[230] Jacob, J. (2020, May 21). *Kerala backs out of Sprinklr deal, cancels controversial pact over privacy issues.* India Today. Available at: https://www.indiatoday.in/india/story/kerala-sprinklr-deal-covid-19-pinarayi-vijayan-high-court-1680484-2020-05-21.

their privacy and autonomy. It further prohibited Sprinkler from using the data for commercial purposes and directed it to return the data to the government after completion of the contractual period.[231] However, the government later cancelled the deal and informed the court that Sprinkler had been directed to destroy all the data.[232]

4.3.2 Tamil Nadu agreement with Google to create patient health records

As reported in November 2022,[233] Google has been engaged by the Tamil Nadu government to help create personal health records (PHRs) of all people in the state. While tech companies have hitherto only worked with private health institutions such as Apollo Hospitals, Aravind Eye Hospitals and Sankara Nethralaya, by offering them free AI in exchange for access to health records, this is the first time, a global tech company has embedded itself with a state health department.

As per the report to build the PHR, the government sought data from 17 databases, such as the public distribution system (PDS) and the Integrated Child Development Scheme (ICDS). Then it generated unique health IDs and linked all other IDs with it. Front line workers collected health and demographic data door-to-door with all of this being digitised. The data is now disseminated across 21 dashboards of different health programmes.

This collection of personal health data and sharing with Google to create PHRs is not only happening absent a data protection law, but not even under terms of a contract. Apparently, the state's National Health Mission (NHM) is currently in the process of finalising a memorandum of understanding (MoU) with Google. In addition to the complete lack of accountability, the terms of the MoU are typically locked under non-disclosure terms jeopardising transparency. Additionally, the data is being collected and allegedly being shared with Google without informed consent of the people without information whether the data is being anonymised, if there are penalties for de-anonymisation, if there is provision for data protection, or whether the terms of the MoU have provisions on commercialisation of data.

Research by Privacy International on PPP reveals common concerns, including "*lack of transparency and accountability in the procurement processes; failure to conduct due diligence assessments; growing dependency on technology designed and/or managed by private companies, with loss of control over the AI applications themselves (to modify, update, fix vulnerabilities, etc.); and over-reliance on the technical expertise of the private company and there are also risk of vendor lock-in. In many cases, the private company supplies, builds, operates and maintains the AI system they deployed, with public authorities not having sufficient knowledge or effective oversight. The lack of an adequate legal framework is often compounded by limited enforcement safeguards provided for in contracts, resulting in limited or no venues for redress.*"[234]

Given the context, going forward, a critical point to consider will be the balance between the increase in value creation by Big Tech and the risk of value capture by monopolies and its consequences. Further, relying on Big Tech will make it difficult for both private hospitals and public health

---

[231] Rahman, F and Shah, A. (2023). State Legibility of Personal Health Data in India. In Parsheera, S. (Ed.). *Private and Controversial: When Privacy and Public Health Meet in India*. Harper Collins.

[232] Jacob, J. (2020, May 21). *Kerala backs out of Sprinklr deal, cancels controversial pact over privacy issues.* India Today. Available at: https://www.indiatoday.in/india/story/kerala-sprinklr-deal-covid-19-pinarayi-vijayan-high-court-1680484-2020-05-21.

[233] Singh, P.V. (2022, November 10). *Why Google is helping an Indian State roll out $300 million healthcare project.* The Ken. Available at: https://the-ken.com/story/why-google-is-helping-an-indian-state-roll-out-a-300m-healthcare-project/.

[234] Privacy International (2021). Our analysis of the WHO Report on Ethics and Governance for Artificial Intelligence for health. Retrieved on April 11, 2023. Available at: https://privacyinternational.org/news-analysis/4594/our-analysis-who-report-ethics-and-governance-artificial-intelligence-health.

departments to protect the personal and social rights of their citizens from the data related practices of these platforms.

In conclusion, digital colonialism can impede a state's capacity to achieve UHC by creating a dependence on foreign digital health platforms, limiting access to affordable digital health solutions, creating unequal digital infrastructure, raising data privacy and security concerns and limiting the capacity for local innovation. It is important for developing countries, such as India, to be mindful of these challenges and strive for inclusive, locally relevant and sustainable digital health solutions to support their efforts towards achieving universal health care.

4.4 Law and policy implications

4.4.1 Competition Law

Governments in several parts of the world, including within the EU, UK, South Korea, and Australia, are considering new laws to curb the market power of a few dominant technology platforms.[235] A US Congress committee report's recommendations include breaking up tech giants, and regulating them better and more proactively,[236] pursuant to which six bills were advanced in June 2021 focusing on the anticompetitive impacts of self-preferencing, mergers and acquisitions, data accumulation, and network effects related to digital platforms.[237]

Google and Apple have faced scrutiny from the Competition Commission of India (CCI), over alleged abuse of the application market. Earlier in 2022, the CCI imposed a penalty of INR 936.44 crore on Google for abusing its dominant position with respect to its Play Store policies, apart from issuing a cease-and-desist order.[238]Apple is potentially facing huge monetary penalties on the similar issue of mandatory use of in-house billing system.[239]

The Parliamentary Standing Committee on Finance has presented a set of recommendations to rein in Big Tech companies through a digital competition law to regulate anti-competitive practices on their platforms, including strict regulation on data usage for advertising. The committee recommended that the companies should be stopped from processing users' data by using services of third parties that utilise their core services.[240]

This has great relevance to health data. Competition law can be useful to regulate the access and use of personal health data by Big Tech companies. For instance, competition authorities can impose

---

[235] Chin, C. (2022, April 22). Breaking Down the Arguments for and against U.S. Antitrust Legislation. CSIS. Retrieved on April 11, 2023. Available at: https://www.csis.org/analysis/breaking-down-arguments-and-against-us-antitrust-legislation.

[236] Subcommittee on Antitrust, Commercial and Administrative Law of the Committee on the judiciary of the House of Representatives, United States of America. (2022). *Investigation of Competition in the digital markets, Part 1*. US Government Publishing Office. Available at: https://www.govinfo.gov/content/pkg/CPRT-117HPRT47832/pdf/CPRT-117HPRT47832.pdf

[237] Ciciline, D. N. (2022, July 19). *Judiciary Committee Published final Report on Competition in the Digital Marketplace.* Press Release. US Congress Rhode Island. Available at: https://cicilline.house.gov/press-release/judiciary-committee-publishes-final-report-on-competition-in-the-digital-marketplace.

[238] Competition Commission of India (2022 October 25). *CCI imposes a monetary penalty of Rs. 936.44 crore on Google for anti-competitive practices in relation to its Play Store policies.* Press Bureau of India. Available at: https://pib.gov.in/PressReleasePage.aspx?PRID=1870819#:~:text=936.44%20crore%20on%20Google%20for,to%20its%20Play%20Store%20policies&text=The%20Competition%20Commission%20of%20India,cease%2Dand%2Ddesist%20order.

[239]Srivats, K.R. (2022, November 6). *A hard bite. After Google, Apple faces anti-trust heat.* Hindustan Business Line. Available at: https://www.thehindubusinessline.com/info-tech/apple-faces-anti-trust-heat-following-google-ruligs/article66103675.ece.

[240] PRS Legislative Research (2022, December 29). *Standing committee Report Summary: Anti-competitive Practices by Big Tech Companies.* PRS. Available at: https://prsindia.org/policy/report-summaries/anti-competitive-practices-by-big-tech-companies.

conditions on mergers and acquisitions, to ensure that use of patient data is in line with competition principles and does not lead to anti-competitive outcomes. Competition law can also promote data portability and interoperability, which could prevent Big Tech companies from creating data silos and restrict competition and consumer choice.

4.4.2 Data protection Law

To promote a competitive marketplace and to protect the right to privacy and autonomy of individuals, it is imperative to enforce data access rules in data protection laws. Special attention should be paid to controlling data access and technology provider usage. There needs to be a careful balance struck between allowing platforms the room to introduce their data-driven innovations to different industries and clearly defining the types of data they can access, combine, and use as well as the additional obligations they must bear when operating in the health sector, in particular. However, as discussed below in Section 5 the proposed legal frameworks for both personal as well as non-personal data, do not address this issue adequately.

4.4.3 Law must address monetisation of health data

As discussed above, the monetization of personal data can have harmful effects on protection of rights – at both the individual and community levels – and can erode informational and decisional autonomy. There is, therefore, an increasing recognition of the urgency to regulate monetisation of data.[241]

The European Data Protection Board (EDPB), in its Guidelines on the processing of personal data in the context of online services[242] states that "*considering that data protection is a fundamental right…, and that one of the main purposes of the GDPR is to provide data subjects with control over information relating to them, personal data cannot be considered as a tradeable commodity.*" The EDPB clarified "*that the processing of personal data differs from monetary payments for multiple reasons, including the fact that, once control over personal data has been lost, it may not necessarily be regained.*"[243] The EDPB and the European Data Protection Supervisor (EDPS) reiterated this position in their Joint Opinion 02/2022 on the Data Act proposal - "*although data subjects can consent to the processing of their personal data, they still cannot waive their fundamental rights*."[244]

In August 2022 the US Federal Trade Commission announced that it is "*exploring rules to crack down on harmful commercial surveillance and lax data security*" and is seeking public comments on the same,[245] specifically relating to "*whether it should implement new trade regulation rules or other regulatory alternatives concerning the ways in which companies (1) collect, aggregate, protect, use, analyze, and retain consumer data, as well as (2) transfer, share, sell, or otherwise monetize that data in ways that are unfair or deceptive.*" [246]

---

[241] Olivi G. & Cairoli, F. (2022, June 13). *The debate over data monetisation - an EU (and Italian) perspective.* Dentons. Available at: https://www.dentons.com/en/insights/articles/2022/june/13/the-debate-over-data-monetization-an-eu-and-italian-perspective.

[242] European Data Protection Board (2019, October 8). *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects.* Available at: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf.

[243] Olivi G. & Cairoli, F. (2022, June 13). *The debate over data monetisation - an EU (and Italian) perspective.* Dentons. Available at: https://www.dentons.com/en/insights/articles/2022/june/13/the-debate-over-data-monetization-an-eu-and-italian-perspective.

[244] European Data Protection Board (2022, May 4). *EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act*). Available at: https://edpb.europa.eu/system/files/2022-05/edpb-edps_joint_opinion_22022_on_data_act_proposal_en.pdf.

[245] Federal Trade Commission (2022, August 11). *FTC Explores Rules Cracking Down on Commercial Surveillance and Lax Data Security Practices.* Federal Trade Commission. Available at: https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data-security-practices.

[246] Ibid.

In India, The NDHM Strategy Overview states that "*certain types of use of personal health data are expected to be prohibited even if the data was provided with consent -- for example usage of data for commercial promotions. A list of such use-cases will be finalised by NDHM in consultation with MoHFW and other stakeholders.*"[247] This needs to be done ~~e~~xpeditiously and addressed in the data protection law for personal and non-personal data. Unfortunately the Digital Personal Data Protection Bill 2022 as well as the proposed framework for regulation of non-personal data steer clear of the monetisation issue. As per news reports, the Digital India Bill being developed by the government will address the issue of monetisation of personal data by Big Tech.[248]

B HEALTH INSURANCE

4.5 Digital health and health insurance

Development of technologies such as wearables, IoT, health bots, drones, and smart appliances have provided insurance companies easy access to a large volume of vital human data. They use this data to further leverage their predictive analysis tools. Predictive analytics is a branch of data analytics that deals with interpreting and analysing data to generate forecasts regarding the risks and probabilities of the events that take place in the future.[249]

Enhanced predictive analysis is utilised for the purposes of claim management, targeted marketing, developing new products and plans, customised and individualised plans, price optimisation, underwriting, and improving customer experience and customer retention – purposes which increase profit margins.[250] As per a survey in 2019, 60% of insurance companies reported that predictive analysis led to increase in sales and profits. Two-third insurers also reported reduction in underwriting and other expenses.[251]

In India, the Insurance Regulatory and Development Authority of India (IRDAI) received 173 proposals (till October 2021), most of which incentivise wellness in the health insurance domain through the use of apps and wearable devices, of which 67 were approved.[252] Some notable product launches include comprehensive app-monitored wellness programmes with wearable devices, especially for lifetime health conditions such as diabetes mellitus.[253]

4.6 Impact on rights

Equitable access to health insurance is a critical component of achieving UHC. It helps ensure financial protection, promotes health equity, increases health service utilisation, supports risk pooling and sustainability, and contributes to health system strengthening. By ensuring that health insurance is available to all individuals in an equitable manner, UHC aims to ensure everyone has access to essential health services without facing financial hardship, regardless of their socio-economic status.

---

[247] MeITY, MoHFW & NHA. (2020). National Digital Health Mission: Strategy Overview. Para no. 2.2.7. Available at: https://www.niti.gov.in/sites/default/files/2021-09/ndhm_strategy_overview.pdf.
[248] Times of India (2023, January 21). Digital India Act will address the issue of monetisation: Union Minister Rajeev Chandrashekhar. TNN. Available at: https://timesofindia.indiatimes.com/india/digital-india-act-will-address-issue-of-monetisation-union-minister-rajeev-chandrashekhar/articleshow/97185915.cms.
[249] "*Predictive modeling in insurance utilizes techniques like data mining, statistics, artificial intelligence, machine learning, deep learning, and more, to analyze and comprehend the large data sets. These findings are then made available in the form of highly detailed reports that highlight the level of risks and other factors that may govern policy formulation and underwriting.*" See Shakeel, F. (2023, March 27). *Top 4 Use Cases of Predictive Analytics in Insurance.* Damco. Available at: https://www.damcogroup.com/blogs/predictive-analytics-in-insurance.
[250] Ibid.
[251] Edwards, M. et al (2020, November 24). *European life insurers are finding analytics treasures.* WTW. Available at: https://www.wtwco.com/en-GB/Insights/2020/11/european-life-insurers-are-finding-analytics-treasures.
[252] Indian Brand Equity Foundation (IBEF). (2023, February 27). *Opportunity for Fintech in the Indian Insurance Industry*. IBEF. Available at: https://www.ibef.org/blogs/opportunity-for-fintech-in-the-indian-insurance-industry.
[253] Ibid

Digital Health technologies leveraging personal data and data analytics is changing the insurance sector which risks undermining equitable access to insurance. Growing surveillance through "wellness" programmes entail serious impact on privacy, autonomy, exclusion and discrimination in insurance and employment settings.

4.6.1 Privacy, autonomy and data security

Surveillance through wearables like Google Fitbits, Apple Watches, Google glasses and other sensors that relay granular updates on how our bodies are functioning is extremely intrusive. Added to this, these wearables can be hacked and personal health data can be stolen. The massive theft of data from some 78 million customers of insurance company Anthem has put the spotlight on security of medical data in the insurance sector, just as wearable technology is growing even more mainstream.[254]

Additionally, as per researchers, wellness programmes which may start as voluntary, are increasingly becoming the norm.[255] This would mean that insurers will start charging higher premiums from consumers who do not share granular data through the wellness programmes. Lower premiums for those who comply and who are deemed low risk, will be offset by charging higher premiums from those considered at higher risk or those who refuse to share granular data. This invasion of privacy will likely result in issues of exclusion and discrimination in the insurance as well as the employment sector.

4.6.2 Changing nature of insurance – exclusions, discrimination, volatility

Insurance grew out of actuarial science, which is based in mathematical models of predictive analysis. These models predict the prevalence of accidents, fires and deaths within large groups of people. The insurance sector, including health insurance, has grown around these predictions, and gave people a chance to pool their collective risk, protecting individuals when misfortune occurred, with insurance companies keeping a portion of the money for themselves, as profit.[256] Now, with granular details of our health including data from our genomes, patterns of our sleep, exercise and diet – insurers will be able to increasingly calculate risk on individual or very small group bases instead of generalities of the larger pool. Insurers are also likely to be able to access and combine granular health details with information such as vehicular insurance and credit scores to further determine risk profiles.[257]

These risk profiles will be used to identify high risk individuals, who will be charged a very high premium or excluded from coverage altogether, where legally permitted. This will exclude the individuals and groups who need insurance coverage the most, by denial or by unaffordability. For others the premiums will become volatile, for example going up every time their blood pressure fluctuates. This is a far cry from the original purpose of insurance, which is to help society balance its risk. In effect instead of paying the average; we end up paying the anticipated cost in advance. This undermines the very point of insurance.[258]

4.6.3 "Wellness" programmes at workplaces – privacy, autonomy, discrimination

Many employers are investing in workplace wellness programmes as a cost-saving measure[259] and several companies are making these mandatory. Employers who opt out or are unable to meet the

---

[254] Riley, C. (2015, February 2015). *Insurance giant Anthem hit by massive data breach.* CNN Business. Available at: https://money.cnn.com/2015/02/04/technology/anthem-insurance-hack-data-security/.
[255] O'Neil, C. (2017). *Weapons of Math destruction*: *How Big Data Increases Inequality and Threatens Democracy.* Penguin Books.
[256] Ibid.
[257] Ibid.
[258] Ibid.
[259] Rajki, S.C. (2009, August). Workplace Wellness Programs: What's Legal, What's Not (and Why Your Company Should Have One). Available at: https://www.sssb-law.com/media/1131/workplace_wellness_programs-_what__s_legal__what__s_not__why_your_company_should_have_one.pdf.

health targets set by the programme are typically required to contribute more towards their premium. These practices erode the right to privacy and autonomy and have discriminatory outcomes on the basis of age, disability etc.[260]

For instance, Scott's Miracle-Gro Company has an aggressive and mandatory workplace wellness programme. Employees who agree to take a health care self-assessment earn a USD 40 per month reduction in their share of insurance premiums. Employees who do not follow the recommendations are required to pay an additional USD 67 a month in insurance premiums.[261]

Michelin, a tire company, sets its employees goals for metrics ranging from blood pressure to glucose, cholesterol, triglycerides, and waist size. Those who don't reach the target in three categories have to pay an extra USD 1000 a year towards their health insurance.[262]

There are also concerns that sharing such granular health data with employers, which they would otherwise not have access to, will enable them to discriminate against individuals on health grounds.

4.7 Laws implicated

According to researchers, in the paradigm of dataveillance, regulations are the only thing that could prevent insurers from using health and fitness data obtained by smartwatches, deleteriously. This necessitates an inquiry in three bodies of law – a) if and to what extent applicable insurance regulations allow for an individualization of insurance contracts; b) whether and under what conditions the individualization is compatible with the requirements of anti-discrimination law; c) access and purpose limitations in data protection law.

4.7.1 Insurance laws

In order to prevent discrimination against individuals and groups on the basis of health status, it is imperative that insurance laws restrict insurance companies from individualising health insurance. For instance, in the USA, under the *Affordable Care Act*, insurance companies can consider only five factors when deciding premiums, namely, age, location, tobacco use, individual versus family enrolment, and proportions of contribution by the insurer and the insured.[263]

In Australia, private health insurers are governed by a community rating system – regardless of health status, age, gender or any other factor, individuals will be charged the same premium as every other member living within their state.[264] The community rating system was developed by the Australian government to make sure that people with a higher level of claims are not disadvantaged – for example, if one has a history of health issues, this does not mean that they should pay a much higher premium. The insurers can, however, offer a discount if they know one is exercising more or eating well. But the governance framework seeks to ensure that the opposite behaviour – someone moving less and eating an unhealthy diet – does not lead to increases in premiums or to the denial of a policy.[265]

---

[260] Ibid.
[261] Ibid.
[262] Supra at 254.
[263] Ho, CWL. (2020). *Ensuring trustworthy use of artificial intelligence and big data analytics in health insurance.* Bull World Health Organ.98(4):263-269. doi: 10.2471/BLT.19.234732.
[264] Henning, L. (2022, July 15). *Wellness apps and fitness trackers: Why insurers love your smartwatch.* The Sydney Morning Herald. Available at: https://www.smh.com.au/business/banking-and-finance/wellness-apps-and-fitness-trackers-why-insurers-love-your-smartwatch-20220712-p5b0y9.html.
[265] Private Health Insurance Community Rating System. Private Healthcare Australia. Available at: https://www.privatehealthcareaustralia.org.au/consumers/private-health-insurance-community-rating-system/.

In India, life insurers can provide individual health policies for a term of 5 years or more, where the premium must remain unchanged for a block of three years minimum. General and health insurers can provide health policies for a minimum of one year and three years at the maximum, where the premium must remain unchanged for the entire term.[266] But there is nothing in law that restricts the number of data points insurance companies can gather to decide premium, to prevent individualisation.

4.7.2 Anti-discrimination laws

With respect to concerns of denial of insurance or discrimination in employment settings due to health status, anti-discrimination laws would be relevant. India does not have an omnibus anti-discrimination law; but with respect to insurance, there is prohibition from discrimination against people living with HIV/AIDS, people with mental health conditions, disabilities and genetic conditions. As per guidelines issued by IRDAI, all insurers must comply with the *Mental Healthcare Act 2017*, the *HIV/AIDS Act 2017 and Rights of People with Disabilities Act, 2016;* [267] and must not deny coverage or claim due to genetic disorders.[268] Every insurer shall make provision for medical insurance for treatment of mental illness on the same basis as is available for treatment of physical illness. With respect to HIV/AIDS, no person shall discriminate against a protected person under the HIV Act, on any ground including the denial of or unfair treatment in the provision of insurance unless supported by actuarial studies.[269]

Similarly, concerns regarding discrimination in recruitment, promotion or unfair termination based on health status can be met by appropriate provisions in anti-discrimination laws.

4.7.3 Data Protection law

In order to prevent insurance companies from using personal health details for their own profits at the cost of individual rights and societal interests, it is important to have provisions in privacy and data protection law, which limits the access to sensitive health data by insurance companies. The proposed Digital Personal Data Protection Bill 2022 does not have any provision to address monetisation or restrict access of insurance companies to health records/EHRs of people. The DISHA Bill 2018 has categorically prohibited insurance companies from having access to EHRs, except for settling of individual insurance claims, but this Bill seems to have been shelved for now. Presently, insurance companies are already offering wellness apps and smartwatches to people with no provisions in law to prevent them from misusing this data.

C PHARMACEUTICAL COMPANIES AND BIG DATA

4.8 Increasing use of digital health technologies in the pharmaceutical sector

Pharmaceutical companies are acquiring personal health information through clinical trials, telemedicine apps, other health apps, wearables like Fitbit, and directly from clinics/hospitals or from EHRs, from big analytics companies, Big Tech such as Google, Microsoft, data mining services, or more recently offering to buy patients information directly from the patients.[270]

These companies seek personal health information for a variety of reasons, including, targeted and direct advertising of drugs and medical devices to patients and doctors, faster and less expensive drug

---

[266] Rule 3, IRDAI (Health Insurance) Regulations 2016.
[267] Dhinesh, S. (2023, March 4). IRDAI Mandates General Insurers to Cover Mental Illness, HIV and PWDs. Enterslice. Available at: https://enterslice.com/learning/irdai-mandates-general-insurers-to-cover-mental-illness-hiv-and-pwds/.
[268] IRDAI circular Reference No.: IRDAI/HLT/REG/CIR/046/03/2018. *Directions of High Court of Delhi at New Delhi on Exclusions Related to Genetic Disorders*. Available at: https://irdai.gov.in/document-detail?documentId=387853.
[269] Section 3, *HIV/AIDS (Prevention and Control) Act 2017*.
[270] Hirschler B. (2018, March 1). Big Pharma, big data: why drugmakers want your health records. Reuters. Available at: https://www.reuters.com/article/us-pharmaceuticals-data-idUSKCN1GD4MM.

discovery and development, improving marketing and sales, developing products and services by predictive analysis and forecasting (for instance diagnostic tools like clinical decision support system (CDSS), which gets embedded in EHRs) and precision medicine.[271] A recent report "Modernising the Pharmaceutical Development Process with EHRs" estimated that EHRs could cut the costs in an average phase 3 clinical trial by USD 5 million.[272]

4.9 The impact on rights and laws implicated

4.9.1 Risks to consent, confidentiality, privacy

Pharmaceutical companies are collecting vast amounts of personal health data from various sources, and the question that arises is whether or not the access they have is consensual. When data is mined, more often than not, people are not aware and when it is sold it is usually not consented to as the data had originally been provided for some other reason. Privacy and confidentiality violations can also occur owing to undesired discovery of embarrassing information about an individual while processing their data. To the extent pharmaceutical companies process special categories of personal data, the risk of suffering a data breach also becomes more significant.[273]

4.9.2 Targeted marketing to consumers undermines consumer choice

In India, Direct-to-consumer (DTC) advertising is mostly for social marketing objectives, such as family planning, health, hygiene, and illness awareness. DTC product promotion is allowed for homoeopathic and patented Ayurveda medications.[274] Such product promotion is prohibited for Schedule H and Schedule X drugs under the *Drugs and Cosmetics Act*. However, due to increased interconnectedness and the nature of the internet, the populace is being increasingly exposed to advertising for prescription drugs, despite legal prohibitions.[275] This is detrimental to people's health as it can lead to consumption without proper consultation, inappropriate usage of antidepressants, overemphasis on potential benefits and not enough awareness about associated risks. Misinformation can lead to creation of an overmedicated society wherein natural conditions, cosmetic issues, or trivial ailments are targeted as issues requiring medical attention.[276]

4.9.3 Direct-to-physician advertising to influence prescribing decisions

DTP through EHRs is the new advertising technique as traditional sales representative access to doctors diminishes. Pharmaceutical companies have a clear incentive to advertise to physicians in EHRs, in order to influence and reinforce their prescribing decisions.

They even tie up with EHR vendors. For instance practice fusion, an EHR vendor company, serves relevant advertisements to physicians from pharmaceutical companies about new therapies, products and services. It has sold two sponsored EHR advisories over the past year, one for vaccinations by Merck ($MRK) and the other for asthma and COPD by AstraZeneca ($AZN).[277] In January 2020, in the first ever criminal action against an EHR vendor, Practice Fusion was ordered to pay a penalty of USD 145 million for soliciting and receiving kickbacks form a major opioid company in exchange for utilising its EHR software, to influence physician prescribing of opioid medication. The press release of the US

---

[271] Ibid.
[272] Bolt, A. et al. Bringing new therapies to patients: Transforming clinical development. Available at: https://www2.deloitte.com/us/en/insights/industry/life-sciences/future-of-drug-discovery.html.
[273] Millar, A. (2021, September 17). Five pharma cybersecurity breaches to know and learn from. Pharmaceutical Technology. Available at: https://www.pharmaceutical-technology.com/features/pharma-cyber-attacks/.
[274] Khosla, P. & Khosla, A. (2011). Direct to consumer advertising of prescription drugs on internet: A Boon or a Curse. Indian J Pharmacol. doi: 10.4103/0253-7613.83128.
[275] Ibid.
[276] Ibid.
[277] Bulik, B.N. (2015, mAY 11). Is there a place for pharma in the emerging EHR market. Fierce Pharma. Available at: https://www.fiercepharma.com/sales-and-marketing/there-a-place-for-pharma-emerging-ehr-market.

Justice Department stated "*the companies illegally conspired to allow the drug company to have its thumb on the scale at precisely the moment a doctor was making incredibly intimate, personal and important decisions about a patient's medical care, including the need for pain medication and prescription amount.*" [278]

The concerns about advertisements on EHRs are the same - that patients may receive suboptimal care if their physician is biased by EHR advertisements and that physicians may under-prescribe less heavily advertised drugs that have better efficacy and/or lower cost.[279] Research shows that exposure to physician-directed advertising is associated with less effective, lower-quality prescribing decisions and that exposure to pharmaceutical company-provided information leads to higher prescribing frequency and higher costs.[280]

Under Indian law, there is prohibition on doctor-centric advertising by way of financial inducements, gifts, sponsorships or donations.[281] A prohibition also exists on engaging pharmacists to advertise a specific medicine to patients.[282] There is however, no obligation to have advertising content approved in advance by a regulatory or industry body.

4.9.4 Data dredging

Data dredging is sometimes described as "*seeking more information from a data set than it actually contains.*"[283] The practice is known by other names as well, such as *fishing trip*, *data snooping* and *p-hacking*.[284] It involves probing data in inadvertent or malicious ways using unplanned analyses till one arrives at the result "so hoped for"; then reporting salient results without accurately describing the processes by which the results were generated.[285] This can prove to be highly risky for the pharmaceutical sector as it could result in false positives and bias, which are then relied upon for research, drug discovery, studying the impact of a drug etc. Placing reliance on unreliable results could prove to be extremely detrimental to human health.

4.9.5 Changing nature of clinical trials and research

Start-ups and Big Tech are actively developing clinical trial solutions, from IoT for remote monitoring and decentralised clinical trials, to machine learning for EHR processing. Decentralised clinical trials (DCTs) make use of digital technologies to enable access of patients to clinical research, remote data collection and monitoring and communication between the investigators and participating subjects.[286] DCTs rely on the use of digital tools such as e-consent apps, wearable devices, Electronic Patient-

---

[278] Department of Justice, Office of Public Affairs. (2020, January 27). *Electronic Health Records Vendor to Pay $145 Million to Resolve Criminal and Civil Investigations.* The United States Department of Justice. Available at: https://www.justice.gov/opa/pr/electronic-health-records-vendor-pay-145-million-resolve-criminal-and-civil-investigations-0.

[279] Harvey KJ, et al. (2005). *Pharmaceutical advertisements in prescribing software: an analysis.* The Medical Journal of Australia. DOI: 10.5694/j.1326-5377.2005.tb06927.x.

[280] Berman, F. et al. (2018). *How drug companies manipulate prescribing behaviour.* Colombian Journal of Anesthesiology 46(4):p 317-321. DOI: 10.1097/CJ9.0000000000000075. Available at: https://journals.lww.com/rca/fulltext/2018/12000/how_drug_companies_manipulate_prescribing_behavior.8.aspx.

[281] Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002; Uniform Code of Pharmaceuticals Marketing Practices (UCPMP). Available at: https://pharmaceuticals.gov.in/sites/default/files/Uniform%20Code%20of%20Pharmaceuticals.pdf.

[282] Pharmacy Practice Regulations, 2015, the Pharmacy Act, 1948. Available at: https://www.pci.nic.in/pdf/Pharmacy%20Practice%20Regulations.pdf.

[283] Awati, R. Data Dredging (data fishing). Tech Target. Available at: https://www.techtarget.com/searchdatamanagement/definition/data-dredging#:~:text=Data%20dredging%20is%20sometimes%20described,not%20have%20been%20discovered%20otherwise.

[284] Ibid.

[285] Erasmus, A. et al. (2022). Data-dredging bias. *BMJ Evidence-Based Medicine* 2022;27:209-211.

[286] Petrini, C. et al. (2022). Decentralised clinical trials (DCTs): a few ethical considerations. Front. Public Health. Available at: https://www.frontiersin.org/articles/10.3389/fpubh.2022.1081150/full.

Reported Outcomes (ePRO), telemedicine, as well as on moving trial activities to the a patient's home (e.g., drug delivery) or to the local healthcare settings (i.e., community based diagnosis and care facilities).[287] The COVID-19 pandemic has caused a significant increase in DCTs [288] and this methodology seems to be poised to take off in India as well.[289]

Big Tech companies are using mobile devices to create platforms that cover the entire clinical trial process. Since 2015, Apple has been constructing an ecosystem for clinical studies around the iPhone and Apple Watch, both of which support the collection of real-time health data.[290] Its open-source frameworks, ResearchKit and CareKit, assist with patient recruitment for clinical trials and remote health monitoring. Almost 500 physicians and medical researchers used Apple's open-source ResearchKit and CareKit software within three years of its release for studies involving more than 3 million participants.[291]

Google, on the other hand, is also building a clinical research ecosystem through its Google Health Studies Android application and its life science subsidiary, Verily Life Sciences, to medical researchers with reams of patient health data that were otherwise difficult to access. Novartis, Sanofi, Otsuka, and Pfizer had partnered with Verily to use its tools for more efficient clinical trials.[292] Google is also working with EHR vendors, to take their systems and data to the cloud, possibly with the objective to incentivise EHR vendors to integrate patient-generated data into Google software.[293]

Clinical research platforms, such as Verily and ResearchKit and decentralised trials in general, implicate a plethora of legal-ethical issues. Substantial regulatory and ethical clarity is needed before such platforms and apps can be considered for use in interventional or randomised trials:

a) One of the main criticisms levelled at the ResearchKit platform is that while trial participants are limited to those who own an iPhone, a whopping 81.5 percent of global smartphone users run Android.[294] This has created a diversity problem for clinical research. Apple users are a population that polls have shown more likely to be richer and better educated than Android users.[295] In a country like India, the problem of diversity becomes more serious, in light of the digital divide, with serious problems for representativeness of clinical trials. This selection bias may affect the ability of researchers to gather good quality data on diseases, which disproportionately affects poorer segments of society.
b) DCTs only have partial application and are not suitable for all medical conditions, therefore its use can only be to supplement traditional means of clinical research/trials.
c) There are risks regarding the validity and reliability of the data collected emanating from the researcher not being with the patients in close physical proximity. There are risks in assuming high participant compliance and formulating disease management conclusions based solely on the data collected by the online platforms. That data from volunteers self-reporting about

[287] Ibid.
[288] Ibid.
[289] Ved, Y. (2021, September 9). India Poised to conduct more decentralised clinical trials : Sanjay Vyas. Pharmabiz.com. Available at: http://www.pharmabiz.com/NewsDetails.aspx?aid=142411&sid=1.
[290] CB Insights (2021, April 6). The Evolution of Clinical Trials: How AI, Big Tech, & Covid-19 Could Make Drug Development Cheaper, Faster, & More Effective. Research Briefs, CB Insights. Available at: https://www.cbinsights.com/research/clinical-trials-ai-tech-disruption/.
[291] Ibid.
[292] Verily signs up four big pharmas to its clinical trials platform. 2023, April 13. Pharmaphorum. Available at: https://pharmaphorum.com/news/verily-signs-up-four-big-pharmas-to-its-clinical-trials-platform/.
[293] CB Insights (2021, April 6). The Evolution of Clinical Trials: How AI, Big Tech, & Covid-19 Could Make Drug Development Cheaper, Faster, & More Effective. Research Briefs, CB Insights. Available at: https://www.cbinsights.com/research/clinical-trials-ai-tech-disruption/.
[294] Dolan, B. (2015, March 13). *In-Depth: Apple ResearchKit concerns, potential, analysis.* Mobi health news. Available at: https://www.mobihealthnews.com/41330/in-depth-apple-researchkit-concerns-potential-analysis.
[295] Ibid.

their symptoms is very susceptible to bias and inaccuracy, which could risk the well-being and safety of the patients. It would also compromise the quality of data which could skew results of the research.

d) DCTs essentially entail electronic consent forms, which raise doubts about consent being easily understandable and truly meaningful in the context of digital divide and digital fatigue.
e) Concerns related to privacy, purpose limitation and function creep also prevail; vast amounts of very granular data is being collected which can even reveal diseases that an individual may not even be aware of. Further, personal information can be used for purposes other than the original purpose of collection, for eg. For direct marketing.
f) There are also risks of monetisation of personal health data. Critics of such platforms are concerned that selling this data to insurance companies may very well be the next step.[296] At present, the profit motive is being kept at arms' length, with the terms and conditions for developers signing up to ResearchKit banning the commercial resale of any data collected. However, there does not seem to be a restriction on, for example, drug companies making an app themselves — provided they get ethics approval — and using the data gathered to profit directly.[297]

One of the main challenges is that the existing regulatory frameworks were designed with conventional clinical trials in mind and may only be partially relevant for DCTs. Moreover, there is guidance on the planning, design and evaluation of DCTs and decentralised methods. And, there are no reference standards concerning the role of ethics committees in the oversight and evaluation of DCTs. An in-depth review of the legal and ethical framework is essential for establishing how existing definitions and conceptual rules for clinical trials are applicable to the decentralised activities of DCTs and how the law needs to be modified to be robustly applicable.

Ethical regulation of decentralised clinical trials is vital for achieving UHC by protecting patients' privacy and safety, ensuring data integrity, promoting equity and access, building trust and acceptance, and promoting compliance and accountability. Ethical conduct of DCTs helps generate reliable evidence for informing health policies and practices, which is crucial for achieving UHC and improving population health outcomes.

The above discussion on health data monetisation practices by Big Tech, insurance and pharmaceutical entities, establishes that unfettered monetisation risks undermining the objective of achieving UHC by compromising privacy and data security; undermining consumer choice and autonomy and patient safety; perpetuating discrimination, exclusion and health inequalities; inequitable distribution of financial benefits derived from data transactions; monetisation of data can lead to the commercialisation of healthcare, where the pursuit of profit may take precedence over public health interests, in turn compromising patient-centred care and divert resources away from addressing the health needs of vulnerable populations and raise ethical conc. To mitigate these risks, it is important to ensure robust data governance frameworks, strengthen institutional and regulatory capacities, prioritise patient privacy and consent, promote equitable distribution of benefits, prioritise public health interest over profit motive, and maintain transparency and accountability in health data transactions.

[296] Mohammadi, D. (2015, May 7). ResearchKit: a clever tool to gather clinical data. The Pharmaceutical Journal. Available at: https://pharmaceutical-journal.com/article/feature/researchkit-a-clever-tool-to-gather-clinical-data.
[297] Ibid.

5 REGULATION OF PERSONAL AND NON-PERSONAL DATA

5.1 Personal data

To date, while there is no privacy and data protection legislation in India, a patchwork of statutes exists that cover some aspects of collection, storage and processing of personal health data. Yet, they are in no way comprehensive.

5.1.1 Statutory recognition of right to privacy of sensitive health data

The Information Technology Act and Rules 2011

The *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011* issued under the eponymous Act, recognise sensitive personal data to include physical, physiological and mental health conditions, sexual orientation and medical records and history, among other things.[298] The rest of the rules lay down the procedure for collecting, storing, processing and sharing this data. However, these rules have several limitations, which underscore the need for a comprehensive privacy and data protection law. For one, all obligations in it apply only to body corporates and not to government bodies and departments. It is out-dated and does not codify all the established privacy and data protection standards, and rights of data principles as recognised under modern data protection frameworks. The rules also do not prescribe any criminal penalties for data breach and exclude intentional breaches, only covering accidental or negligent ones.

HIV/AIDS (Prevention and Control) Act, 2017

All establishments keeping records of a person's HIV-related information, are required to adopt data protection measures. These measures include procedures for protecting information from disclosure and for authorised access, as well as data security measures and mechanisms to ensure accountability and liability of persons in the establishment.[299] The draft National AIDS Control Program Data Management Guidelines 2020 prohibits sharing of PII with any third party for research purposes.[300] However, both the HIV/AIDS Act and the draft guidelines are not comprehensive enough to contend with the volume and speed of data collection, processing and sharing that is being envisaged in India and already occurring, particularly in the private sector. The Act also does not codify the necessary privacy and data protection principles as well as the data rights of people, and hence is not adequate to protect the right to privacy of people living with HIV/AIDS.[301]

5.1.2 Supreme Court judgment on the fundamental right to privacy

In 2017, a nine-judge bench of the Supreme Court of India, in the landmark judgment of *Justice K.S. Puttaswamy (Retd) v Union of India*, unanimously reaffirmed that the right to privacy, including privacy of health/ medical data, is a fundamental right inherent in the fundamental right to life and personal liberty under Article 21 of the Constitution.[302] As per the judgment, medical privacy involves *informational privacy* (including confidentiality, anonymity, secrecy and security of health data), *physical privacy* (including modesty and bodily integrity); *associational privacy* (including intimate sharing of death, illness and recovery), *proprietary privacy* (including self-ownership and control over personal identifiers, genetic data, and body tissues), and *decisional privacy* (including autonomy and choice in medical decision-making).

---

[298] Section 3, *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011*.

[299] Section 11, *HIV/AIDS (Prevention and Control) Act, 2017*

[300] National AIDS Control Organisation (2020). *National AIDS Control Programme Data Management Guidelines 2020*. Available at: http://naco.gov.in/sites/default/files/Draft%20NACP%20Data%20Management%20Guidelines%202020.pdf.

[301] Divan, V. and Rai. S. (2023). Confidentiality and HIV/AIDS: The need for humaneness and precision in the law. In Parsheera, S. (Ed.). *Private and Controversial: When Public Health and Privacy Meet in India.* Harper Collins. pp. 181-199.

[302] (2017) 10 SCC 1

Additionally, the court held that privacy is also the necessary condition precedent to the enjoyment of any fundamental rights and freedoms, such as those to life, dignity, freedom of speech and expression and equality.

As a crucial point that underscores the importance of privacy for public health, the court held that protection of privacy is important for individual rights as well as for achieving the collective well-being of the community. This observation resonates with the experience in relation to the HIV/AIDS epidemic, which established that confidentiality and privacy of health data builds trust in the medical community, encourages people to seek testing and treatment for themselves, and get the information & tools necessary to prevent further transmission, thereby fulfilling their own rights, as well as the community interest, and goal of public health to control a pandemic.

The court laid down the test for examining infringement of the right to privacy. Any encroachment to privacy of medical data a) must be backed by a law b) the law itself must pursue a legitimate aim, c) should be a rational method to achieve that aim, d) must be the least restrictive alternative; and e) have safeguards from abuse.

The court particularly emphasised the importance of informational privacy in the ubiquitous digital age and expressed grave concerns about the dangers of both an Orwellian State riding on Big Data and data capitalism at the hands of private actors. Therefore, it called for enactment of ***a comprehensive data protection law***, codifying privacy and data protection standards and rights of users.

5.1.3 Digital Personal Data Protection Bill 2022

After the 2017 *Puttaswamy* judgment, MeitY tasked the Justice BN Srikrishna Expert Committee to review concerns related to data protection and propose a draft law for India. The committee released a report with a draft Bill in July 2018.[303] Following a round of public consultations, MeitY introduced a revised version of the draft Bill before the Lok Sabha in December 2019. On introduction, the Bill was referred to a Joint Parliamentary Committee (JPC) for deliberation, which released its report and a further revised version of the draft law in December 2021.[304] However, in August 2022, MeitY withdrew that draft by citing the JPC's concerns on precision in drafting and stated that it was undertaking renewed efforts at presenting a draft Bill to comprehensively deal with data protection. In December 2022, MeitY introduced the latest version for public consultation – the Digital Personal Data Protection Bill, 2022 (DPDP Bill).[305]

The DPDP Bill is an omnibus data protection law. There are a few notable developments that mark a departure from previous iterations of the proposed law, which are of concern. The definition of 'sensitive personal data' is deleted from the latest bill, with no explanation offered for this decision. This has crucial implications for several provisions of the Bill. For instance, the 2021 Bill defined sensitive personal data to include health data, biometric data and genetic data, among other categories, and specified that such data will not be processed for purposes of employment. Now with the dispensation of any qualitative distinction between personal data and sensitive personal data, the

[303] Ministry of Electronics and Information Technology (2018), A Free and Fair Digital Economy Protecting Privacy, Empowering Indians, Committee of Experts under the Chairmanship of Justice B.N. Srikrishna. Available at: https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf.

[304] Lok Sabha (2021), Report of the Joint Committee on the Personal Data Protection Bill. Available at: https://prsindia.org/files/bills_acts/bills_parliament/2019/Joint_Committee_on_the_Personal_Data_Protection_Bill_2019.pdf.

[305] Ministry of Electronics and Information Technology (2022), MEITY invites feedback on the draft 'Digital Personal Data Protection Bill, 2022'. Available at: https://www.meity.gov.in/writereaddata/files/Notice%20-%20Public%20Consultation%20on%20DPDP%202022_1.pdf.

restrictions on processing of health data for employment purposes stand completely removed. This can grant unguided access and discretion to employers to process health data that has no bearing on recruitment, performance assessment or termination of individuals.

The DPDP Bill states that it applies only to personal data, which is collected online or digitally. This leaves ungoverned a trove of personal data which is collected and stored offline, and intended to form part of a filing system (whether digitised or otherwise). A large amount of sensitive personal data being collected may or may not be digitised, such as that collected by frontline health workers (ASHAs) from individuals to make family health cards under the Ayushman Bharat scheme. The collection of such offline data must also be protected by the law.

A corollary of the aforesaid point is the right to object to automated decision-making. The HDMP provides that the system of digital health records is voluntary. In this backdrop, it bears well to note whether the DPDP Bill's framework of processing personal data will permit submission of paper-based documents/IDs if an individual objects to automated processes, which is recognized as a right under progressive international legal frameworks on data protection.[306]

Another aspect missing in the DPDP Bill is accountability. The users' right to compensation for any data breaches, as was proposed in earlier iterations is not provided in this draft. This is recognised as part of the international legal framework on the right to privacy and included in the data protection laws of other countries.[307]

5.1.3.1 Preamble

The DPDP Bill's preamble states its twin objectives as 1) processing digital personal data for lawful purposes and 2) protection of digital personal data. The preamble is illustrative of the structural imbalance of power through which the proposed law will govern digital privacy of individuals. However, it does not explicitly recognise the right to privacy as a fundamental as held in the *Puttaswamy* judgment. Yet, it needs to be explicitly stated that the judgment is the guiding basis for the processing of personal data under the proposed law and to ensure that the decision-making processes provided under it are circumscribed by the rigours of the *Puttaswamy* standard.

5.1.3.2 Purpose limitation & notice

The DPDP Bill reduces the important principle of "purpose limitation" to a "ground" for processing personal data.[308] The law must ensure as a matter of principle that the specific purposes for which personal data are processed should be explicit, legitimate and determined at the time of collection of personal data. The explanation for "lawful purposes" being "*any purpose which is not expressly forbidden by law*" is overbroad, vague and arbitrary, and invalid as per settled law.[309] Instead, the Bill needs to codify the rule on purpose limitation appropriately as one that must be followed as a mandatory duty by data fiduciaries rather than to operate as a routine ground for processing of personal data.

---

[306] Article 22 of the GDPR provides data subjects with a right not to be subject to decisions solely based on automation, including profiling, which produce legal effects concerning the individual.

[307] For example, the *UK GDPR 2022* gives data principals the right to seek compensation if their personal data has been breached due to a Company's security failures. Article 18 of the EU GDPR gives the right to claim compensation if any person suffers material or non-material damage as a result of an infringement. Under the *Australian Privacy Act 1988*, individuals have the right to make complaints to the Privacy Commissioner if they believe that their privacy has been breached by an organisation. If the Privacy Commissioner, upon investigation, finds that there has been a privacy breach, the Commissioner has the power to make a determination that certain remedies be provided to the individual whose privacy has been breached, including requiring the organisation to pay compensation to the individual whose privacy has been breached.

[308] Section 5, draft DPDP Bill 2022.

[309] *Shreya Singhal v Union of India* (2015) 5 SCC 1

5.1.3.3 Consent framework

Section 7 of the DPDP Bill states that consent must be "*freely given, specific, informed and unambiguous indication*" of the data principal's wishes for processing his/her personal data. However, it does not define what constitutes informed consent as provided in earlier iterations of the draft law. For one, the explanation must state that the "specified purpose" is explicit, legitimate and that personal data will not be further processed in a manner that is incompatible with the specified purpose, as also provided under the EU GDPR.

Further, the provision explicitly states that the consequences of withdrawing consent will be borne by the individual. This puts people at risk of being denied any service despite providing limited information necessary for delivery of that service. In 2021, the Delhi High Court held that policies that operate in a "*take it or leave it*" paradigm are unconstitutional in so far as such practices virtually force individuals into agreement with service providers.[310]

Section 8 permits consent of data principals for processing of personal data through an overbroad mandate, including "*the performance of any function under any law, or the provision of any service or benefit to the Data Principal*" and "*for the purposes related to employment*", among other grounds. In contrast, Article 88 of the EU GDPR requires more rigorous standards that reflect a priority given to protecting the data principal's rights – while allowing member States to make specific rules for processing data for employment, it enjoins them to include measures to safeguard human dignity and rights of employees. The 2019 Bill restricted data processing for employment to specific purposes. As section 8 stands, virtually every person who avails any government service or is employed in the public or private sector can be compelled to provide '*sensitive personal data*' without any restriction. The exceptional power to process any personal data through deemed consent of individuals may be constitutionally invalid for violating the *Puttaswamy* standard of proportionality.

Specifically in relation to health, the government has the authority to process personal data during medical emergencies, public health measures during an epidemic and provision of services during a disaster. It is neither clear what constitutes a medical emergency involving threat to the health of individuals, nor what constitutes threat to public health or breakdown of public order. Any such provision must be specific and clearly define the contours within which personal data may be shared. The ostensibly welfare-oriented provisions do not dispense the State's duty to comply with the *Puttaswamy* standard on proportionality, as reiterated in the matter of COVID-19 vaccine mandates.[311]

5.1.3.4 Exemptions

Section 18 of the DPDP Bill exempts the government "*from the application of provisions of this Act*" for the processing of personal data for '*national security*' grounds. This may violate the proportionality standard as laid down in the *Puttaswamy* judgment. Exceptions to fundamental rights mandates necessitate that they be narrow, otherwise their validity is questionable as disproportional.

The aforesaid exemption relates to processing of personal data in interests of grounds relating to sovereignty and integrity of India, security of the state, friendly relations with foreign states, maintenance of public order and the prevention of offences relating to national security grounds. As far as grounds relating to maintenance of public order and prevention of offences relating to national security grounds are concerned, they appear to be valid since both grounds are inextricably linked to occurrence of actual events and thus narrowly tailored.

[310] *Whatsapp LLC v Union of India*. Delhi High Court. LPA 163 of 2021.
[311] *Jacob Puliyel v Union of India* 2022 SCC OnLine SC 533

However, the inclusion of the national security grounds as stand-alone grounds *per se* is disproportionate as each ground is severed from a real and imminent threat and thus grants unwarranted powers to authorities. The manner in which 'national security' grounds are generally conceived to be invoked under the DPDP Bill for processing of personal data raise particular concern with respect to arbitrary exercise of power and the need for safeguards. Settled law dictates that an act which poses a real and imminent threat to national security must be a precondition for restriction of rights by authorities as per law.[312] Thus none of the stand-alone national security grounds are legally sustainable.

Further, the procedure established by law for processing of personal data for prevention of offences relating to national security must be fair, just and reasonable in order to mitigate the misuse of power. This includes recording reasons in writing for invoking such extraordinary powers instead of adopting alternative measures which seek informed consent and are least restrictive, stipulation of an expiry period of such exercise of power and the destruction of records after necessity for such purpose has ceased, among other safeguards as per the standards laid down in the *PUCL* and *Puttaswamy* rulings.

Additionally, settled law mandates that mere invocation of 'national security' as a ground in prevention of offences is manifestly arbitrary and amenable to judicial review.[313] The government must justify invoking such power by providing material to illustrate the existence of a real and imminent threat before a court, as also mandated in other foreign jurisdictions. [314]

Section 18(3) exempts data fiduciaries from the requirement of taking consent and complying with general obligations having regard to the "*volume*" and "*nature of personal data*". This will apply to data fiduciaries processing small amounts of data. However, all businesses are vulnerable to security threats. Available evidence indicates that smaller organisations are targeted more as they have poor cyber security protocols and governance, and are more likely to capitulate to ransom in order to get the data or control over their operations back – 82% of attacks in 2021 impacted organizations with less than 1,000 employees.[315] Any law considered by the parliament should, therefore, clearly stipulate the minimum privacy and data security measures applicable to all organisations irrespective of volume and nature of personal data, which the DPDP Bill fails to do.

Section 18(4) exempts "*any instrumentality of the state*" from the duty to cease retention of personal data when there is no purpose for the same. As this provision sanctions storing of personal data without consent for 'national security' grounds in perpetuity, it is disproportionate and thus constitutionally untenable.

5.1.3.5 Governance and enforcement

A fair data protection regime requires establishment of an independent statutory authority answerable to the parliament, to deal with the contraventions of the data protection framework as well as to proactively supervise its compliance by both State and non-State actors. The proposed governance structure under section 19 lacks clarity on all these aspects.

This section leaves the size, composition, selection process, tenure, terms and conditions of appointment and terms of removal to be determined by delegated legislation. Under section 19(3), the chief executive officer of the Data Protection Board will be determined and appointed by the central government. In order to serve transparency and accountability, these terms and conditions

[312] *People's Union for Civil Liberties (PUCL) v Union of India* (1997) 1 SCC 301
[313] *Manohar Lal Sharma v Union of India* 2021 SCC Online SC 985
[314] *Fred Korematsu v United States of America* 584 F. Supp. 1406 (1984)
[315] Law enforcement pressure forces ransomware groups to refine tactics in Q4, *Coveware* (2021). Available at: https://www.coveware.com/blog/2022/2/2/law-enforcement-pressure-forces-ransomware-groups-to-refine-tactics-in-q4-2021.

should be clearly laid out in the Bill itself, and not left to the discretion of the government. Indeed, such an approach will tend to ensure that the Board will function as an independent authority, free of pressures exerted by the government.

In particular, due consideration should be given in determining the composition of the Board. The Bill provides for the collection, storage, protection and sharing of personal data of individuals. This task is complex and evolving, and entails striking a balance between facilitating sharing of data for legitimate purposes and ensuring the privacy and security of individual personal data. The Data Protection Board must not only comprise expertise from various fields such as technology, privacy and cyber security, but also representatives of the public such as consumer and patients' rights advocates and groups.

Any regulatory authority performs legislative, executive and adjudicatory functions, and these functions must be clearly specified in the statute.[316] Section 20 falls short on this ground - other than determination of cases of non-compliance, remaining functions are left to the wide discretion of the government.

It is imperative that paramount regard be given to the need for transparency in the conduct of any regulator while carrying out its functions. While there may be some specific decisions or deliberations of the regulator that may not be released immediately, this should not be unduly used as a reason to deviate from the general principle of transparency. Section 20 should therefore require the Data Protection Board to publish all its decisions, be transparent about meetings and when any information is kept confidential, record the reasons for doing so.

5.1.3.6 Amendment of RTI Act

Section 8(1)(j) of the RTI Act is an important accountability measure which has revealed information relating to tax evasions by public officials,[317] opened up the highest constitutional offices to provide information on assets of functionaries,[318] and generally developed a culture of transparency in functioning of public officials at all levels.[319]

The DPDP Bill proposes an amendment to section 8(1)(j) of the *Right to Information (RTI) Act, which* is wholly contrary in spirit to the recommendation of the BN Srikrishna Committee Report. The report recommended amendment of this clause in order to clarify the limited grounds for disclosure of personal information which has any public interest, thereby balancing the privacy of the individual with the underlying purpose of the provision, i.e., promoting transparency in public affairs. The committee also proposed another amendment for the section by adding an overriding clause with respect to a data protection law, in order to ensure that "*privacy does not become a stonewalling tactic to hinder transparency.*"[320]

However, the drafters of the DPDP Bill wholly misconceive recommendations of the report, in so far as the provision is sought to be reduced to a complete bar on access to personal information, irrespective of its value in addressing concerns of accountability in public affairs. Therefore, the

---

[316] Committee of Experts under the Chairmanship of Justice BN Srikrishna (2018). *A Free and Fair Digital Economy Protecting Privacy, Empowering Indians*. Government of India. Available at: https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf; FSLRC (2013). *Report of the Financial Sector Legislative Reforms Commission (Volume 1)*. Government of India. Available at: https://dea.gov.in/sites/default/files/fslrc_report_vol1_1.pdf.

[317] *Yamaji Sakharam Rathod v CIT, Aurangabad* CIC/AT/A/2007/00009

[318] *Central Public Information Officer, Supreme Court v Subhash Chandra Aggarwal* (2020) 5 SCC 481

[319] *Vijay Prakash v Union of India* AIR 2010 Del 7

[320] Committee of Experts under the Chairmanship of Justice BN Srikrishna (2018). *A Free and Fair Digital Economy Protecting Privacy, Empowering Indians*. Government of India (pp. 102-105). Available at: https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf.

proposed amendments to section 8(1)(j) are a direct attack on transparency and cast doubt on the *bona fide* intent of the Bill.

5.2 Non-personal data

Secondary use of health data usually alludes to processing of non-personal health data for purposes other than the primary purpose of providing direct patient care. Secondary use of health data for public health purposes includes analysis, research, quality and safety measurement, certification or accreditation, epidemiological research, and to strengthen understandings about effectiveness of health care systems. As such, secondary use of health data provides an important resource for decision-making, health system management, improvement, and research.[321] Secondary use also includes monetisation of health data. However, as discussed previously, there is increasing recognition that indiscriminate monetisation of health data in the private sector is threatening the right to health, privacy and non-discrimination and must therefore, be circumscribed.

The ABDM facilitates secondary use of health data by both government (for public health purposes) and private entities (for public health as well as commercial activities). The mission also facilitates sharing of publicly held datasets within government departments and with private entities. Complex ethical, political, technical, and social issues surround the secondary use of health data, which play increasingly critical and complex roles given current public and private sector activities with health data (as discussed in earlier sections).[322] Data sharing underscores the importance of certain prerequisites such as having strong cybersecurity and data protection laws, identifying and placing safeguards from abuse, and having appropriate frameworks for classifying data categories.[323]

Different jurisdictions around the world are experimenting with legal and governance frameworks in an attempt to balance the privacy and security of non-personal data while promoting the benefits from secondary uses of such data. Germane to law and policy considerations are challenges related to limits to anonymisation, addressing monetisation, recognition of individuals and communities as producers of health data, and ensuring their autonomy over collection and sharing of anonymous data and for what purposes. Some researchers point out that India could do well to learn the following lessons from Finland before rushing to set up data sharing mechanisms: a) Finland adopted the GDPR (legal framework) before setting out on data sharing mechanisms; b) It employed a more robust consultation and feedback mechanism; c) It progressively developed digital, infrastructural, institutional and regulatory capacity, while learning continually from their process. Data sharing framework has emerged from several pilot studies, tests and evidence, over a period of time lending to policy maturity. As a result, it reflects focus on individual & community data rights, data protection, ownership, interoperability, technical and human capacity, sectoral decision-bodies & conditions for access and evidence-based legislation.[324]

5.2.1 Central and state government policies on sharing non-personal data

While the DPDP Bill to regulate personal data was still in the works and a legal framework for non-personal data was being mulled over, the government of Karnataka notified its Open Data Policy in October 2021. Close on its heels, MeitY released the Draft India Data Accessibility and Use Policy in February 2022. The objective of both the policies was three-pronged – to promote effective management and interoperability for sharing of data across state and central government

[321] WHO (2021). Support tool to strengthen health information systems. Available at: https://www.who.int/europe/publications/i/item/9789289055741

[322] Safran, C. et al (2007). Toward a national framework for the secondary use of health data: an American Medical Informatics Association White Paper. J Am Med Inform Assoc. doi: 10.1197/jamia.M2273.

[323] The World Bank (2021). World Development Report 2021: DATA FOR BETTER LIVES. https://www.worldbank.org/en/publication/wdr2021

[324] Kapoor, A. (2023). Data Stewardship: solutions for sharing of health data. In Parsheera, S. (Ed.) *Private and Controversial: When Public Health and Privacy Meet in India.* (page nos.). Harper Collins. pp. 266-286.

departments; define processes and standards for enabling proactive open access to government held data for research, innovation and evidence-based governance by other entities; and monetise anonymised citizen data.

These policy moves were critiqued as being premature on two counts,[325] First, in the absence of a data protection law, the opening up of non-personal data for various purposes raised the spectre of infringement of privacy by both government departments and private actors. No jurisdiction has mandated data sharing without placing a privacy and data protection law first.

Second, the government's headlong dive into data sharing without doing the assessment and preparedness towards infrastructural, institutional and governance capacity, structures and processes necessary for a responsible and successful data governance framework. India has had an Open Data sharing policy among government sectors since 2012, namely the National Data Sharing and Accessibility Policy (NDSAP), which obligated sharing non-personal data to foster innovation. However, the policy failed to gain pace due to reasons of poor uptake by government departments, poor data quality and inadequacy and copyright and licensing issues.[326] The government ought to carry out an assessment, identify gaps, make a plan of action, conduct pilot tests and generate evidence (for example, on interoperability), clarify sectoral decision-making (for example, for health data), which would inform current debates as well as policy formulation.

Several jurisdictions – the EU, Australia, UK, Singapore and Finland – have taken many years before adopting data-sharing, adopted data protection laws first, carried out robust consultations, used case and impact assessments, and pilot studies to generate evidence, before introducing frameworks for sharing of non-personal data.[327] This has helped in achieving policy maturity, placing checks and balances and grievance redress mechanisms appropriately, constituting a prerequisite for data sharing.[328]

Both the Karnataka and MeiTY policies seem to have skipped consent and failed to delineate purposes for which data will be shared. Instead, the government department harnessing the data will become the 'owner' of it, and decide how it should be shared with other departments or private entities. Hence, citizens would not know how, why, and by whom their data is being processed, undermining decisional autonomy and privacy.

The policies continue to erroneously assume that anonymised data is fully privacy preserving and further fail to prescribe the standards and thresholds for data anonymisation. This could lead to the use of methods such as pseudonymisation, where personal identifiers are replaced with pseudonyms instead of being anonymised.[329] The EU's GDPR recognises pseudonymised data as personally

[325] Internet Freedom Foundation (IFF). Comments on Draft India Data Accessibility & Use Policy, 2022. Available at: https://internetfreedom.in/the-government-wants-to-sell-your-data/; Gurumurthy, A. & Chami, N. (2021, October 28). *Monetising Data: For whose good?.* Deccan Herald. Available at: https://www.deccanherald.com/opinion/in-perspective/monetising-data-for-whose-good-1044830.html; Sridharan, S. & Narayan, V. (2022, March 24). *Karnataka's Open Data Access: At what cost?*. The Data Economy Lab. Available at: https://thedataeconomylab.com/2022/03/24/karnatakas-open-data-access-at-what-cost/

[326] Bailey, R. et al. (2022). Comments on the draft India Data Accessibility and Use Policy, 2022 http://dx.doi.org/10.2139/ssrn.4080917

[327] Supra at 324

[328] Thejesh, G.N. (2020). *'Open Data in India: In a Restrictive Copyright Regime, Voluntary Organisations Pitch in to Make Data Accessible',* Economic and Political Weekly.

[329] "*What differs pseudonymisation from anonymisation is that the latter consists of removing personal identifiers, aggregating data, or processing this data in a way that it can no longer be related to an identified or identifiable individual. Unlike anonymised data, pseudonymised data qualifies as personal data under the General Data Protection Regulation (GDPR). Therefore, the distinction between these two concepts should be preserved.*" Zerdick, T. (2021, December 21). *Pseudonymous data: processing personal data while mitigating risks.* European Data protection

identifiable data.[330] Notably, the UK's NHS was criticised for using pseudonymisation instead of anonymisation in its data sharing contracts with private companies, and had to suspend its contract with Palantir for the same reason.[331]

The monetisation of publicly held data risks creating perverse incentives for governments who may be willing to sell increased amounts of data in exchange for boosting their revenues, ignoring the privacy and data rights of their citizens.[332] More importantly, "*without a vision of public data as a vital public policy instrument that can incentivise innovation by smaller players, there is a real risk that open public data will end up servicing a few dominant players of the platform economy who have already locked up the social commons of data.*"[333] This in turn, could undermine the objective of using health data for public health purposes and innovation, and equitably distributing the value of data to genuinely benefit the communities who produce the data.[334] The EU's *Data Governance Act* clearly highlights that though public sector bodies should be able to charge some fees for the re-use of data, it is equally important to make the data available at lower or no cost for certain categories of re-use, such as non-commercial re-use, or re-use by small and medium-sized enterprises.[335]

The policies also smacked of lack of transparency. For instance, the agreement between the Karnataka government and private entities will be covered under a non-disclosure agreement, which will shroud important information such as the prices at which data is sold, the purpose for which it will be used, the parties involved, and accountability measures in secrecy As has been critiqued, "*The role of individuals and communities as producers of data is obscured, making their participation in data-sharing decisions impossible*."[336]

In June 2022, MeitY released The Draft National Data Governance Framework Policy, seemingly to replace the previous Draft India Data Accessibility and Use Policy. In a significant change from the previous policy, it seems to have dropped the monetisation proposal. It has now proposed development of a public data infrastructure called the 'India Datasets Program' and goes a step further to suggest that in addition to government data, privately held data is also required for its successful development. This has been appreciated by stakeholders as a welcome move given that "*most important and extensive data in almost every sector is held by a few corporations that own and control large customer-facing digital platforms.*"[337] However, stakeholders also expressed concerns that the private sector would not "voluntarily" share data that gives it comparative advantage and market dominance with the government. Voluntary data sharing, therefore, is critiqued as a "*major logical fallacy because no reasonable economic actor would willingly give up control of its most important resource,*" leave alone corporations with their profit-maximising motives.[338]

Supervisor. Available at: https://edps.europa.eu/press-publications/press-news/blog/pseudonymous-data-processing-personal-data-while-mitigating_en

[330] European Commission. What is personal data? Available at: https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en#:~:text=Personal%20data%20that%20has%20been,the%20scope%20of%20the%20GDPR.

[331] Shead, S. (2021, October 11). *UK government ends one of its data contracts with Palantir.* CNBC. Available at: https://www.cnbc.com/2021/09/10/uk-ends-one-of-its-data-sharing-contracts-with-palantir.html

[332] Gurumurthy, A. & Chami, N. (2021, October 28). *Monetising Data: For whose good?.* Deccan Herald. Available at: https://www.deccanherald.com/opinion/in-perspective/monetising-data-for-whose-good-1044830.html

[333] Ibid.

[334] Sridharan, S. & Narayan, V. (2022, March 24). *Karnataka's Open Data Access: At what cost?*. The Data Economy Lab. Available at: https://thedataeconomylab.com/2022/03/24/karnatakas-open-data-access-at-what-cost/

[335] European Commission. Shaping Europe's Digital Future. The Data Governance Act explained. Available at: https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained

[336] Sridharan, S. & Narayan, V. (2022, March 24). *Karnataka's Open Data Access: At what cost?*. The Data Economy Lab. Available at: https://thedataeconomylab.com/2022/03/24/karnatakas-open-data-access-at-what-cost/

[337] See IT for Change's response to The Draft National Data Governance Framework Policy. Available at: https://itforchange.net/inputs-from-it-for-change-to-meity-on-draft-national-data-governance-framework-policy

[338] Ibid.

5.2.2 JPC recommendations on regulation of non-personal data

In July 2020, the Expert Committee constituted by the MeitY published a draft report for public consultation. The Committee observed that non-personal data should be regulated to (i) enable a data-sharing framework to tap the economic, social, and public value of such data, and (ii) address concerns of harm arising from the use of such data.[339] Based on the feedback received from this consultation, the Committee released a revised version of the draft for public consultation in December 2021.

The proposed framework suffers from the same shortcomings as the preceding policies – no impact assessment of its previous and contemplated initiatives, assumes anonymisation as irreversible, does not lay down standards or thresholds for anonymisation, takes consent only for anonymisation and not for subsequent sharing of data, and does not address the issue of data monetisation by private entities. The report also fails to lay down the specific purposes for which data should be shared. All these shortcomings create a recipe for misuse of data.[340]

Additionally, although the proposed framework mentions community rights in data, it is vague on its structures, processes and mechanisms. Design and implementation of data trustees is vague as it does not adequately clarify the mechanisms through which communities can ensure that their data is used for public good and not just be commodified for private profit. Therefore, while the intention to create bottom-up structures is well placed, the enablement is unclear.[341]

Finally, data sharing must be decentralised at different levels and for different purposes, and capacities of states in governance and management must be built.[342] States and cities could be playing an increasingly important role in data use and management given their proximity to and understanding of community-driven uses of data.[343] For instance, Barcelona through the DECODE project implemented citizen-led data sharing to make data more accessible to local communities and businesses. In one effort, Barcelonians shared anonymised environmental sensor data from their homes — encrypted through the DECODE technology — with community groups to better engage with their city government. This enabled citizen autonomy and control over the reuse of their data for purposes and with entities as determined by them.[344]

6. KEY RECOMMENDATIONS

This paper concludes that unless the deployment and governance of digital health technologies is firmly anchored in human rights law and ethics frameworks, it will erode progress towards UHC, instead of facilitating it. This section makes certain policy and legal recommendations that are necessary to align the adoption of law and policy as well as deployment of digital health technologies, with India's obligations under human rights law (rights to confidentiality, privacy, autonomy, health, equality and non-discrimination, equity, participation and grievance redress); and principles of sound evidence-based public health policy (impact assessments, digital health technology assessment and institutional preparedness).

---

[339] Kapoor, A. (2020, December 30). *Data for development: Revisiting the non-personal data governance framework.* Observer Research Foundation. Available at: https://www.orfonline.org/expert-speak/data-development-revisiting-non-personal-data-governance-framework/

[340] Ibid.

[341] CUTS International (2021), *Navigating the Puzzle of Non-Personal Data Sharing: Three-Pronged Analysis of Rationale and Assumptions.* , Jaipur, India. Available at: https://cuts-ccier.org/pdf/report-navigating-the-puzzle-of-npd-sharing.pdf

[342] Supra at 324

[343] Supra at 341

[344] Mohamed, S. (2020, September 10). *Cities & Data Sharing — Part 3: Barcelona.* The Data Economy Lab. Available at: https://thedataeconomylab.com/2020/09/10/cities-data-sharing-part-3-barcelona/

1. Technology is not a substitute for well-functioning health systems

As evidenced during deployment of digital contact tracing apps, telemedicine and CoWIN, there are significant limitations to what technology is able to resolve. Digital technology is at best complementary to existing service delivery mechanisms. While big data analytics and AI can potentially enhance health systems and support the realisation of UHC, such technology cannot replace the fundamental components of the health system, which include the health workforce, service delivery, leadership and governance. Therefore, investment in digital health technologies must not deviate resources away from health system strengthening.

2. The adoption and deployment of digital health technologies must be anchored in the rights-based framework, namely international human rights law and fundamental rights on privacy, health (availability, accessibility, acceptability and quality), non-discrimination and equity to minimise the significant harms associated with their deployment. The government must operationalise the guidance issued by WHO which states that "*for AI to have a beneficial impact on public health and medicine, ethical considerations and human rights must be placed at the centre of the design, development, and deployment of AI technologies for health*" (including human rights by design and human rights impact assessments).

3. The Digital Personal Data Protection Bill 2022

The DPDP Bill, 2022 must follow the standards laid down by the *Puttaswamy* judgment, i.e., all restrictions to privacy must be rooted in legitimate state interest, proportional to the object sought to be achieved and provide for safeguards to prevent misuse. Some specific deficiencies in the Bill that the government should address include:

a) It treats all kinds of data on an equal footing. Instead, it should classify data as sensitive personal data and personal data, and add health data including genetic data in the former category. This distinction is imperative because of its implications on health data processing for employment, commercial use, public health, national security, etc. Earlier iterations of the bill provided this distinction and limited its access;
b) Provide comprehensive notice and consent provisions for explicit, opt-in and granular consent
c) Adopt all the internationally and domestically recognised[345] privacy, data protection principles, transparency principles, privacy by design requirement and users' rights. These include purpose limitation, data minimisation, right to correction, erasure, information, explainability, object to profiling and automated decisions making, breach notification and the right to be compensated for data breaches etc.
d) The assumption of deemed consent for certain kinds of data processing is overbroad and should be limited, including the obligation to be specific to a particular instance of data processing; and,
e) The regulatory authority should be clearly defined, including checks and balances to ensure its independence and accountability.

4. Non-Personal Data Governance framework

a) Carry out a Regulatory Impact Assessment (RIA) as a prerequisite to a legal framework – It is imperative to consider the functionality of the NPD Governance Framework in the context of challenges of infrastructure, capacity, adequate safeguards, trust, inadequacies already faced by the existing data sharing initiatives in India, including the National Data Sharing and Accessibility Policy (NDSAP), and different regulatory approaches and its impact on individuals and communities. It should learn from the experiences of superimposing a novel governance structure over weak institutional capacities negating transparency, and accountability frameworks among citizens, industry, market, and the state.

[345] *Justice K. S. Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1

b) Consultative and transparent – The government must hold public consultations with relevant stakeholders, including civil society and communities and must make their methodology public.
c) Clear and precise legal framework – No country has initiated data sharing without an existing privacy legislation. Data sharing needs to be anchored in individual data protection and privacy law, in which
   - The purpose for data sharing must be clear from the outset, and data should only be collected to answer clear, pre-defined questions.
   - Individuals must be able to consent dynamically (granularly) **t**o the collection/use of their data, and to grant and withdraw consent as needed.
   - When determining the data sharing for sovereign purposes/public interest, these must be defined narrowly and justifiable only on the three-pronged test of proportionality, legality, and necessity laid down in the *Puttaswamy* judgment.[346]
   - Anonymisation – Since approximately 99.98% of anonymized data may be capable of re-identification it no longer supports the binary categorization into personal and non-personal data.[347] At the very least the law must have clear definitions, standards and thresholds of 'anonymisation' coupled with criminal penalties for de-anonymisation.
d) Federalism and data sharing – Data sharing cannot be a centrally managed and controlled exercise. It has to happen at different levels for different purposes, with states, cities, local authorities playing an increasingly important role in data use and management given their proximity to and understanding of community-driven uses of data. Focus must be on supporting states in developing their institutional and infrastructural capacities in data governance. This is important as more and more states are getting into public private partnerships with technological companies.
e) Democratic and decentralised data sharing governance models – Data sharing must ensure that individuals and communities can exercise control over how and for what purpose their data is used. Models of participatory governance are being developed that need to be further studied and analysed in the Indian context before adoption
   - The DECODE project, piloted in Amsterdam and Barcelona, is an example of such participatory data governance. Public agencies created an infrastructure that made data available for social benefit use, whilst still allowing individuals to retain control over whether their data can be shared, with whom, and for what purposes.[348]
     There are several examples of data trusts and data cooperatives that ensure individuals and communities can steer the use of their data for common good.

5. Health Data Monetisation – In light of the dangers to consent, autonomy and privacy of health data,[349] anti-competitive practices adopted by Big Tech,[350] and the impact on competition, affordability & equity, the following are recommended:

a) The NDHM strategy overview states that *"certain types of use of personal health data are expected to be prohibited even if the data was provided with consent -- for example usage of data for commercial promotions. A list of such use-cases will be finalized by NDHM in*

---

[346] *Justice K. S. Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1
[347] Luc Rocher, Julien M. Hundrickx & Yves-Alexandre de Montjoye, "Estimating the success of re-identification in incomplete data sets using generative models" (2019) 10 *Nature Communications* 3069
[348] https://decodeproject.eu/
[349] Copeland, R. and Needleman, S.E. (2019, November 12). Google's Project Nightingale Triggers Federal Inquiry. Wall Street Journal. Available at: https://www.wsj.com/articles/behind-googles-project-nightingale-a-health-data-gold-mine-of-50-million-patients-11573571867; Lomas, N. (2020, December 10). France fines Google $120M and Amazon $42M for dropping tracking cookies without consent. Available at: https://techcrunch.com/2020/12/10/france-fines-google-120m-and-amazon-42m-for-dropping-tracking-cookies-without-consent/
[350] *United States v Google Inc*., No. CV 12-04177 SI.

consultation with MoHFW and other stakeholders."[351] This needs to be done expeditiously and addressed in the data protection law.

b) Monetisation of not only personal but non-personal data must be regulated:
   - Since the difference between personal and non-personal is no longer substantial.
   - It can prop up data monopolies, which might be better able to afford datasets, than smaller players such as smaller companies, independent researchers and civil society organisations. This will undermine the objective of socio-economic equity, which should be the basis of data sharing.
   - It creates perverse incentives for governments to prioritise revenue maximisation over duty of preserving privacy.

6. Public Private Partnerships in digital health – A moratorium on PPP in digital health must be declared until legislative frameworks on data protection are in place. Alternatively, a) there should be oversight of vetting of PPPs b) central and state governments must include unambiguous clauses on type of data being shared, obligations to ensure privacy, data protection, organisational and technological mechanisms, in contracts; and c) contracts should not be under non-disclosure terms to ensure transparency and public scrutiny.

7. AI and machine learning in health – In its 2021 report on the ethics and governance of AI in healthcare, WHO emphasised the potential health disparities that could emerge due to AI. Medical care is plagued by inequalities and inequities on grounds of sex, gender, age, race, ethnicity, income, education and geography which are codified in data sets. AI algorithms trained on these data sets will further entrench discrimination against already marginalised communities. There is also evidence that AI can be unreliable, make diagnostic errors, is opaque and comes with serious privacy concerns. Hence, there is a need to develop legislation regulating all facets of application of AI and machine learning in health. Further, ethical and human rights considerations should be mandated during the design, development, and deployment of AI technology, including transparency, explainability and auditing of algorithms.

8. Cybersecurity law and strategy – The Indian government needs an overall and sector-specific cybersecurity strategy. Foremost, like in the US, the Indian government should classify health and public health as critical-information infrastructure under section 70 of the *Information Technology Act 2000*.[352] Second, the government should overhaul the regulatory framework for preventing and managing cyberattacks, providing for stricter standards and robust monitoring and enforcement. The National Cybersecurity Policy 2013, is outdated and ill-equipped to deal with the kind of threats posed today. The government should publish its new and updated policy, as promised by the Prime Minister in 2021. Finally, the Ministry of Electronics and Information Technology, in consultation with the National Health Authority, should develop and publish a cybersecurity strategy for the health sector, including financial support and IT training for the healthcare workforce at all facilities.

9. Health technology assessment – India should develop a legal framework to carry out 360-degree assessment of digital and data-driven health technologies, including parameters on ethics, human rights, and equity. The United Nations has recommended employing health technology assessment frameworks to digital health technologies.[353] The National Institute of Health and Care Excellence in the UK has been continuously developing standards to assess the effectiveness and value of a variety

[351] National Digital Health Mission Overview. Para no. 2.2.7

[352] Critical-information infrastructure refers to computer resources whose destruction or incapacitation will have a debilitating impact on national security, economy, public health or safety. All sectors or industries classified as critical-information infrastructure must ensure enhanced protection of its data systems.

[353] UNDP (2021). Guidance on the rights-based and ethical use of digital technologies in HIV and health programmes. UNDP (p. 10). Available at: https://www.undp.org/publications/guidance-rights-based-and-ethical-use-digital-technologies-hiv-and-health-programmes.

of digital health technologies.[354] Until such time, the government must do an evaluation of the digital health tools already deployed on efficacy, privacy and access to health and equity parameters. The government must as a priority conduct a rigorous evaluation of the *Aarogya Setu* application on effectiveness and also enable independent researchers to do the same.[355] This is imperative to advance evidence-based decision-making en route to UHC.

10. Digital divide – Digital divide is a major hindrance in the ability of individuals to interact with digital health services. Even though digitalisation comes with numerous opportunities, the inability to access and benefit from it acts as a caveat, depriving individuals and communities of enjoying the positives of technology. If gaps in digital healthcare infrastructure are not addressed, it can further exacerbate existing socio-economic inequalities. Digital health literacy and internet connectivity have recently been acknowledged as "*super social determinants of health*" in that they have implications for the wider social determinants of health.[356] For this, the government will need to ensure availability of low-cost and continuous internet and mobile devices throughout the country but especially in rural and hard to reach areas; facilitate financially sustainable digital literacy campaigns for marginalised populations, such as women, elderly and low-caste communities; and ensure content on the internet is available in local languages.

11. Ayushman Bharat Digital Mission – First and foremost, the ABDM should be supported with a data protection law along with rules specific to health data. It cannot be emphasised enough that the HDMP, the governance framework underpinning the HDMP, is simply not enough. It does not constitute an independent regulatory body and does not contain adequate safeguards to ensure that digitization of medical records is undertaken with due protection of individual autonomy, informed consent, confidentiality and privacy. Further, it simply states that liabilities and penalties will be as per existing law. However, absent a data protection law, the current laws simply do not have adequate penalties to cover different actors and different ways in which data can be breached. Apart from an absent legal framework, inadequate health system preparedness cast doubt on the overall sustainability, scalability and adaptability of the system. It is imperative that the identified shortcomings are addressed as soon as possible. To this extent, active and sustained stakeholder engagement will provide a strong feedback loop to aid in the development of the programme.

12. Digital health applications – Analysis of the various digital health applications highlights key lessons that must be incorporated in the design and deployment of all health apps, namely:

a) Participation in any health app must be premised on individual autonomy and voluntariness, and under no circumstances lead to denial of services for refusal to join the app.
b) The design and development of any health app must incorporate key privacy principles including purpose limitation, data minimisation, accuracy of data, storage limitation and adequate security measures. All these aspects must be contained in the privacy policy in specific terms.
c) The design and development of any health app must include widespread public engagement. Feedback from public engagements must feed back into the design and deployment strategy of the app.

---

[354] See, NICE (2019). Evidence Standards Framework for Digital Health Technologies. Available at: https://www.nice.org.uk/about/what-we-do/our-programmes/evidence-standards-framework-for-digital-health-technologies; NICE (2019). Highly specialised technologies guidance. Available at: https://www.nice.org.uk/about/what-we-do/our-programmes/nice-guidance/nice-highly-specialised-technologies-guidance.

[355] WHO & ECDC (2021). Indicator framework to evaluate the public health effectiveness of digital proximity tracing solutions. WHO. Available at: https://apps.who.int/iris/bitstream/handle/10665/341818/9789240028357-eng.pdf?sequence=1&isAllowed=y.

[356] Sieck, C. J., Sheon, A., Ancker, J. S., Castek, J., Callahan, B., & Siefer, A. (2021). Digital inclusion as a social determinant of health. *Npj Digital Medicine*, *4*(1). Available at: https://doi.org/10.1038/s41746-021-00413-8

d) The privacy policy of health apps must clearly specify users' rights including the rights to access, object, erasure, rectification, information, explanation, portability and the choice not to be subject to automated decision-making. The app developers must clearly inform users about these at the time of enrolment.
e) All health apps must be transparent and accountable to its users. The privacy policy of the app must clearly specify the name and contact details of its grievance redress officer, as well as lay down the redressal process in the policy itself.
f) The design and deployment of health apps must be helmed by epidemiologists and public health experts.
g) All health apps must undergo a 360-degree evaluation which not only looks at the efficiency and effectiveness of the app, but also assesses it on key privacy, ethical, social and cultural dimensions. This must be done prior and after the rollout of the app.

13. Inclusive and widespread public engagement – Policies defining and establishing governance parameters for the digital health ecosystem are not only vital to protect against the risks of digitisation, but also for reaping its benefits to the fullest extent. However, public engagement on the various policies defining ABDM and digital health technologies has been opaque, purely online and limited. In many cases, the time given to the general public to comment on proposed policies has been much shorter than the one-month time period prescribed under the Government of India's Pre-Legislative Consultation Policy 2014. Moreover, the notice for public consultations has not been adequately disseminated to reach out to as many people as possible and limited to the extent of responding to specific questions as contained in the consultation document. The consultative process has also been conducted purely online. For meaningful and widespread public engagement in the process, it is imperative that all consultation documents should be widely disseminated in print and electronic media and such other manner that may be necessary to reach all affected communities. This must be accompanied with an explanatory note on key provisions of the draft policy in simple language, its financial implications, and an estimated assessment of its likely impact on various stakeholders, followed with sharing a summary of comments or feedback received from all stakeholders in the public domain, as well as how the various comments have been incorporated in the final policy. Consultation should not be limited to written form, but comprise oral consultations with all stakeholders.