AFPI Karnataka Newsletter

Issue: Volume 4, Issue 2

Ethical challenges of digital health technologies: Aadhaar, India

Vijayaprasad Gopichandran (Employees State Insurance Corporation Medical College and Post Graduate Institute of Medical Sciences and Research, Chennai, India)

Parasuraman Ganeshkumar (Indian Council of Medical Research, National Institute of Epidemiology, Chennai, India)

Sambit Dash (Department of Biochemistry, Melaka-Manipal Medical College, Manipal Academy of Higher Education, Karnataka, India)

Aarthy Ramasamy (Madras Diabetes Research Foundation, No. 4, Conran Smith Road, Gopalapuram, Chennai, 600086, India)

Introduction

Low- and middle-income countries have experienced a rapid and massive influx of digital and mobile technologies and their applications. This information and communication revolution has brought great benefits for the practice of public health in these countries. Several studies have shown evidence of effective digital applications in health including electronic health records, digital epidemiology and mobile health applications.[1] With these massive strides in digital health, important ethical issues related to the collection, storage, use and dissemination of patients' digital health information arise.

The *Aadhaar* (Hindi, meaning foundation or base) system of India provides each citizen with a unique identification number, linked to demographic and biometric information about the individual. The National Health Mission established the health management information system across various states of the country, where everyone is also provided with a unique health identification number. Linking this unique health identification number with the *Aadhaar* system has been proposed; merging the digital identification system with digital health care records could enable greater efficiency in investigating public health, conducting relevant research, ensuring the accuracy of health-related information and monitoring welfare programmes.[2] However, the availability of big data in health care, particularly in low- and middle-income countries, introduces unique challenges. We identify and discuss such challenges in this article.

Local setting

The delivery of health care in India is characterized by a vast public health infrastructure, which is categorized into primary, secondary and tertiary care services, delivered by the government-funded health system and a private health sector. The public health system is funded by tax revenues and state-sponsored health insurance schemes, such as *Ayushman Bharat*, and the private health system is largely financed out of pocket and, to a small extent, by private health insurance. In recent years, digital health records have penetrated the public as well as private health systems; most public health data are now recorded in digital format. One of the major issues faced by the public health sector in India is inadequate funding and inefficient utilization of the funds allocated. The enhancement of currently available digital health records will greatly increase the efficiency of planning and budgeting for the health care services.

Approach

Under the Unique Identification Authority of India, established under the Ministry of Electronics and Information Technology of the Government of India, the *Aadhaar* system provides a 12-digit unique identification number to every Indian resident who chooses to enrol as per the provision of the *Aadhaar* (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.[3] The *Aadhaar* identification system records demographic data such as name, address, date of birth and sex, but also biometric data including ten fingerprints, two iris scans and a facial photograph.[4]

Identification by *Aadhaar* number yields several important advantages in development and welfare programmes in the country. Targeted interventions, such as subsidies, cash benefits and incentives provided by the state can reach the intended beneficiaries without pilferage or loss. The *Aadhaar* system has been increasingly linked to bank accounts, income tax accounts, mobile phone numbers, and social welfare programmes, such as disability and elderly pension schemes.

Relevant changes

Since 2013, *Aadhaar* has also been linked to several health-related schemes.[2] For example, the Maternal and Child Tracking System is an electronic database that records information about pregnant women in India, including details of antenatal care, delivery and child-related data up to immunization. A conditional cash transfer programme (*Janani Suraksha Yojna*) encourages women to undergo delivery in a health facility by providing a direct benefit transfer; combining this cash transfer programme with the Aadhar identification system ensures that the correct person receives the benefit.

Other national health programmes, such as the Revised National Tuberculosis Control Program and the National AIDS Control Program, have recently started linking their databases with Aadhaar.[2] The intended benefit of linking the patient databases to the *Aadhaar* number is to track the treatment of patients and ensure that any interruptions to treatment schedules or non-compliance is identified and acted upon. However, interruptions in the treatment of patients with tuberculosis were reported due to pressures to link their treatment registration numbers with their *Aadhaar* identification number.[5] There have also been several reports of HIV-positive patients and patients with AIDS who were undergoing antiretroviral therapy but, fearing a breach of their privacy by allowing their *Aadhaar* number to be included in the AIDS treatment programme documents, they preferred to drop out of the treatment programme.[6]

Lessons learnt

The summary of main lessons learnt is presented in Box 1.

Box 1. Summary of main lessons learnt

- Use of the *Aadhaar* identification number in health programmes in India has met with mixed success due to patients' fears of loss of privacy.
- The proposed merging of the *Aadhaar* identification system with other digital health databases in India could enable greater efficiency in monitoring public health, but important ethical issues of data use and protection must be considered.
- Low- and middle-income countries must invest in developing strict legal regulations to protect data and avoid its exploitation for profit.

Linking sensitive private health information with the *Aadhaar* identification system introduces issues of potential breaches of privacy, data ownership and use, and the autonomy of individuals whose data have become available for analysis. Unlike the United Kingdom of Great Britain and Northern Ireland and the United States of America, who have strong data ownership and protection laws, India has the evolving Electronic Health Record Standards of 2016, which does not have the force of law. Data are owned by the state in a sense of stewardship in the United Kingdom and by the individual in the USA. The Indian Electronic Health Record Standards stipulate that data are owned by individuals, but the state is the custodian of these data. This provision implies that any use of electronic health records requires the authorization of the individual. The exceptions to this rule are situations of emergency and epidemics, in which case the state can collect information without permission. Where data are shared without consent, this is only in a completely anonymized form.[7]

The *Aadhaar* identification system has been the subject of several litigations in various courts in India. In a ruling in 2013, the Supreme Court of India clearly ruled that registering for an *Aadhaar* identification number is voluntary and that nobody should be denied benefits and services because they do not have an *Aadhaar* number. Despite this ruling, several national health programmes continue to enforce *Aadhaar* registration in subtle ways. For example, although including an individual's *Aadhaar* number is not compulsory in many public health programmes, some health workers continue to insist on this. If patients refuse, the health worker can delay or even prevent the receipt of benefits. In 2017, the Supreme Court ruled that the Right to Privacy is fundamental. This ruling reignited the various debates on the constitutional position of the *Aadhaar* system and whether it is an infringement of the privacy of individuals. In 2018, the Supreme Court upheld the constitutional position of Aadhaar, but ruled again that it is not mandatory.[8] However, in the absence of strong regulation of electronic health records in low- and middle-income countries, linking sensitive health information to the *Aadhaar* system results in the privacy of patients being compromised.

Other major ethical concerns regarding the linking of digital health data and *Aadhaar* identification data are the safety and protection of the combined database. Many low- and middle-income countries do not yet have the required data protection laws; even if such laws are present, implementation can be difficult to monitor. Leaks of the *Aadhaar* data have been reported; a private telecommunication company in India collected the *Aadhaar* numbers of many of its subscribers and published them on the internet. Over 200 government websites were also found to be inadvertently displaying *Aadhaar* data of individuals.[9] Although these websites have been taken down, such data can remain in the digital world indefinitely and continue to compromise the privacy of an individual.

Linking digital health data with the *Aadhaar* identification system also facilitates the exploitation of the data for profit. Some technologists who were initially involved in the establishment of the *Aadhaar* system are now working in private for-profit companies. Although security measures are in place to prevent this conflict of interest, there are several loopholes in these regulations.[10] When such profit-motivated, digitally empowered multinational companies gain access to an identification database in low- and middle-income countries, this disproportionately affects the poor and vulnerable. Effective security systems and strong legislation are required to ensure that private companies do not profit from accessing such databases. In this context, the Ministry of Electronics and Information Technology tabled the Draft Personal Data Protection Bill, 2018. When passed, this bill will set up a national Data Protection Authority to supervise and regulate those who collect data, ensuring the autonomy of individuals.[11]

Low- and middle-income countries are joining the digital revolution, making big data available for potential health applications. However, weak health data protection laws and evolving data protection capabilities in these countries leave the population vulnerable to serious ethical consequences, such as breaches in privacy and loss of autonomy. In examining the merging of *Aadhaar* identification data with digital health data in India, we have demonstrated the need for strong health data protection laws to preserve and protect the fundamental human right: that of privacy.

1. Wyber R, Vaillancourt S, Perry W, Mannava P, Folaranmi T, Celi LA. Big data in global health: improving health in low- and middle-income countries. Bull World Health Organ. 2015 Mar 1;93(3):203–8. http://dx.doi.org/10.2471/BLT.14.139022 pmid: 25767300↩

2. Abraham R, Bennett ES, Sen N, Shah NB. State of Aadhaar. Report 2016-17. New Delhi: IDInsight; 2017. Available from: https://stateofaadhaar.in/assets/download/State-of-Aadhaar-Report_2016-2017.pdf [cited 2019 Jan 17].↩

3. What is Aadhar. New Delhi: Unique Identification Authority of India; 2019. Available from: https://uidai.gov.in/your-aadhaar/about-aadhaar.html [cited 2019 Dec 2].↩

4. Ministry of Law and Justice (Legislative Department). The *Aadhaar* (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act. New Delhi: Unique Identification Authority of India; 2016. Available from: https://uidai.gov.in/images/targeted_delivery_of_financial_and_other_subsidies_benefits_and_services_13072016.pdf [cited 2019 Dec 2].↩

5. Rao M. Aadhaar made mandatory for TB patients seeking cash assistance from the government. Scroll.in. 2017 Jun 21. Available from: https://scroll.in/pulse/841250/aadhaar-made-mandatory-for-tb-patients-seeking-treatment [cited 2019 Dec 5].↩

6. Rao M. Why Aadhaar is prompting HIV positive people to drop out of treatment programmes across India. Scroll.in. 2017 Nov 17. Available from: https://scroll.in/pulse/857656/across-india-hiv-positive-people-drop-out-of-treatment-programmes-as-centres-insist-on-aadhaar [cited 2019 December 2].↩

7. Electronic health record (EHR) standards for India. New Delhi: Ministry of Health & Family Welfare; 2016. Available from:

https://mohfw.gov.in/basicpage/electronic-health-record-ehr-standards-india-2016 [cited 2019 Dec 2].↩

8. Safi M. Indian court upholds legality of world’s largest biometric database. The Guardian. 2018 Sep 26. Available from: https://www.theguardian.com/world/2018/sep/26/indian-court-upholds-legality-of-worlds-largest-biometric-database [cited 2019 Dec 2].↩

9. Press Trust of India. Over 200 govt websites made Aadhaar details public: UIDAI. The Times of India. 2017 Nov 19. Available from: https://timesofindia.indiatimes.com/india/210-govt-websites-made-public-aadhaar-details-uidai/articleshow/61711303.cms [cited 2019 Aug 22].↩

10. Thaker A. The new oil: Aadhaar’s mixing of public risk and private profit. The Caravan. 2018 May 1. Available from: https://caravanmagazine.in/reportage/aadhaar-mixing-public-risk-private-profit [cited 2019 Dec 2].↩

11. The Personal Data Protection Bill. New Delhi: Ministry of Electronics and Information Technology; 2018. Available from: https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf [cited 2019 Dec 2].↩