Weighing in on a health data retention plan

A privacy-centric process is needed to determine what data to retain and for how long

RISHAB BAILEY, HARLEEN KAUR, BRINDA LASHKARI & AMEYA ASHOK NAIK

In a welcome development, the National Health Authority (NHA) – the body responsible for administering the Ayushman Bharat Digital Mission (ABDM) – has initiated a consultation process on the retention of health data by health-care providers in India (https://bit.ly/3uK9buH). The consultation paper asks for feedback on what data is to be retained, and for how long.

A simple classification system, as suggested in the consultation paper, exposes individuals to harms arising from over-collection and retention of unnecessary data. At the same time, this kind of one-size-fits-all system can also lead to under-retention of data that is genuinely required for research or public policy needs. Instead, we should seek to classify data based on its use. In this system, health data not required for an identified purpose would be anonymised, or deleted.

The need for such a policy

Whether the state should mandate a retention period at all is an open question. Currently, service providers can compete on how they handle the data of individuals or health records; in theory, each of us can choose a provider whose data policies we are comfortable with. Given the landscape of health-care access in India, including through informal providers, many patients may not think about this factor in practice. Nonetheless, the decision to take choice out of the individual's hands should not be taken lightly.

The Supreme Court of India has clarified that privacy is a fundamental right, and any interference into the right must pass a four-part test: legality; legitimate aim; proportionality, and appropriate safeguards. The mandatory retention of health data is one such form of interference with the right to privacy.

In this context, the question of legality becomes a question about the legal standing and authority of the NHA. For instance, the consultation paper asks whether the health data retention policy should be made applicable only to health-care providers who are participating in the ABDM ecosystem, or to all health-care providers in general. We believe the answer can only be the former; since the NHA is not a sector-wide regulator, it has no legal basis for formulating guidelines for health-care providers in general.

Balancing benefits and risks

The aim of data retention is described in terms of benefits to the individual and the public at large. Individuals benefit through greater convenience and choice, created through portability of health records. The broader public benefits

GETTY IMAGES/ISTOCKPHOTO

through research and innovation, driven by the availability of more and better data to analyse.

While these are important benefits, they do have to be weighed against the risks. Globally, legal systems consider health data particularly sensitive, and recognise that improper disclosure of this data can expose a person to a range of significant harms. These could include harms that would be very difficult to make whole, so it is not enough to have penalties for such breaches; every effort must be made to minimise the extent of data collected, and to hold it only for the amount of time needed so as to reduce the likelihood of any breach in the first place.

In particular, privacy risks should make us very hesitant about retaining an individual's entire health or medical record on the grounds that they might be useful for research someday. As per Indian law, if an individual's rights are to be curtailed due to anticipated benefits, such benefits cannot be potential or speculatory: they must be clearly defined and identifiable.

This is the difference between saying that data on patients with heart conditions will help us better understand cardiac health – a vague explanation – and being able to identify a specific study which will include data from that patient. It would further mean demonstrating that the study requires personally identifiable information, rather than just an anonymous record – the latter flowing from the principle of proportionality, which requires choosing the least intrusive option available.

In fact, standards for anonymisation are still developing. In a world of big data, the research community is still to arrive at consensus on what constitutes adequate anonymisation, or what might be considered best practices or methods for achieving it. We are not yet able to rule out the possibility of anonymised data still being linked back to specific individuals. In other words, even anonymisation may not be the least intrusive solution to safeguarding patients' rights in all scenarios.

Possible safeguards

Ultimately, the test for retaining data should be that a clear and specific case has been identified for such retention, following a rigorous process run by suitable authorities. A second safeguard would be to anonymise data that is being retained for research purposes – again, unless a specific case is made for keeping personally identifiable information. If neither of these is true, the data should be deleted.

An alternate basis for retaining data can be the express and informed consent of the individual in question. However, there are limits to how consent can apply in the context of health care in India; in general, health care is a field where patients rely on the expertise and advice of doctors, making the idea of informed consent complicated. Further, if consent is made necessary for accessing state-provided services, many people may agree simply because they lack any other way to access that care.

Finally, health-care service providers – and everyone else – will have to comply with the data protection law, once it is adopted by Parliament. The current Bill already requires purpose limitation for collecting, processing, sharing, or retaining data; a use-based classification process would thus bring the ABDM ecosystem actors in compliance with this law as well.

Rishab Bailey is a lawyer and technology policy researcher based in New Delhi. Harleen Kaur is a regulatory affairs and public policy lawyer practising in a Delhi-based law firm. Brinda Lashkari is a Policy Associate at eGovernments Foundation, Bengaluru. Ameya Ashok Naik is Head of Policy and Advocacy at eGovernments Foundation, Bengaluru