DRiefcase's user base has 2,500 families comprising some 4,000 to 5,000 individuals

Digital wellness

A great chasm of unsecured medical data prevents India from realising its dream of taking health care online, finds **Nikita Puri**

A few years ago, when Harsh Parikh's uncle travelled to India from the US and fell ill, he had to be taken to hospital. But it was a struggle for the Parikh family to share his medical records with the physician. They were all on paper, and not all with him.

"Sometimes it is a major issue like this. At other times there are minor irritants, like forgetting your child's vaccination charts at home when you've taken her to the doctor. These made us realise the necessity of digitising health records," say Mumbai-based entrepreneurs Parikh and Sohit Kapoor. The former investment bankers quit their jobs and started DRiefcase, a patient-centric record-keeping online platform.

For DRiefcase's user base of 2,500 families — comprising some 4,000 to 5,000 individuals — medical records are available on any device and can be pulled up for reference or shared with a doctor in minutes. Electronic health records have only been around for a short while in India, but in two shakes of a lamb's tail, they've already emerged as a gamechanger for patients and doctors alike.

When Anil Kumar, professor and head of medicine at the Bengaluru-based M S Ramaiah Hospitals, wants to check on his patients, he picks up a tablet — the device, not medication. His patients' vital data can be accessed through a service provided by Stasis, a Bengaluru-based start-up that monitors six vital signs of patients in critical care units. Likewise, Devi Prasad Shetty, cardiac surgeon and founder of the Bengaluru-based Narayana Health chain of hospitals, uses Microsoft's Kaizala app to access his patients' medical records.

Digital records have a significant role to play even in India's tryst with telemedicine. In a report titled *Digital India: Technology to transform a connected nation*, the McKinsey Global Institute found India could save $4-5 billion every year by implementing telemedicine techniques, including doing away with paper records.

But even as some platforms use sophisticated encryption to ensure that a person's medical data is safe, there lies a great divide between their services and how that data is handled.

Take, for instance, the snafu India saw a few weeks ago when Ukraine-based cyber security researcher Bob Diachenko stumbled on the fact that one state government in India had left 12.5 million medical records unprotected on their website — not even a password was required to gain access to them. The records were of pregnant women. Dating back to five years, they included ultrasonography results, genetic tests of foetuses, and details of surgical procedures. The data had names, telephone numbers and residential addresses of the patients, besides details of their doctors. After Diachenko reached out to the government hospital, it took three weeks for the data to be taken down. Since the website's server is still vulnerable, Diachenko only identifies the portal as belonging to "a state in North India".

If only this was a one-off error. "Data breaches and security lapses are a continuous affair in India," says Srinivas Kodali, an independent cyber security researcher from Hyderabad. "They happen because there's no law to safeguard against them. Data security requires some investment. No one bothers until something serious happens."

In 2018, Kodali sounded an alert when he found that a website run by the Andhra Pradesh government allowed anyone with an internet connection to track state-run ambulances in real time. From pick-up and drop-off points to why the ambulance was called (assault, heart attack, and so on), significant details were available to everyone. In another instance, an unsecured government website listed everything everyone had purchased at a government-run store. Everything from erectile dysfunction medication to anti-nausea drops were on this list alongside names and contact details of those who had bought the medication.

When it comes to medical data, "one has to assess who has access to it and what really constitutes sensitive data. These questions have to be answered as data gets continuously hoarded by different platforms," says Roheet Rao, vice-president, sales and marketing, Stasis.

"The moment a patient comes into India's healthcare system, they are left without the knowledge of what personal data is gathered and to what extent it will be used," says Apar Gupta, a Delhi-based lawyer and executive director of the Internet Freedom Foundation. And this is not true only of upscale private hospitals, where digital is a holy cow as one would expect, but in major government-run facilities such as Delhi's All India Institute of Medical Sciences and Chandigarh's PGIMER. Hospitals such as these are not just attempting to up their digitisation but promote telemedicine too.

"In the instance that there's a violation of any kind, people lack any meaningful recourse or remedy because there's no law or institutional authority when it comes to this data. This is especially worrying for India when it is embracing digitisation in all modes," says Gupta.

Last year, a draft for DISHA, or the Digital Information Security in Healthcare Act, was opened up for consultation. Though the draft in its current form still leaves a lot to be desired, experts feel it could pave the way for better handling of healthcare, if lawmakers take into account feedback they've received. But this draft in itself is dependent on the Draft Personal Data Protection Bill of 2018 and could take a couple of years to kick in.

In the meantime, it is imperative to understand that the impact of such lapses is far-reaching. "The data can be used to collect information for organ trade or even target patients disproportionately with insurance premiums," says Kodali. "If these were anonymised and aggregated data sets, that could help pharma companies, but individual data sets is a breach of privacy," say Kapoor and Parikh of DRiefcase.

DRiefcase employees who visit homes to scan medical records and upload them online (a service the company offers because they found that the reason people were not digitising their records was "mainly inertia") are police-verified. And the company's computer and scanning systems are encrypted to ensure there's no data breach. Stasis, too, has strict authentication protocols for doctors and nurses, besides data encryption.

There's little relief in the fact that India is not alone in trying to keep up with advancements in digital space and the security protocols that need to grow with it. In March, for instance, Dutch cyber expert Victor Gevers reported that a portal in China had left open an unsecured list of more than 1.8 million women with the age, education, marital status and contact details of each along with a column marked "BreedReady". The deplorable column gave out contact details of women between the ages of 18 and 95. This is significant at a time when China is dealing with a glaring gender gap and an even more serious crisis of falling birthrates now that it has abandoned its one-child policy.

One reason the government collects data is to ensure better healthcare for its people. Security lapses often happen, say experts, because the data is trading so many hands in an unsecured way. But a significant amount of control lies in the hands of patients, too. "A lot of people are using personal medicare apps these days," says Kodali. These could be tracking one's calorie intake, diet and exercise patterns. "We really don't know where this data is stored and if it is being shared with others."

The Wall Street Journal recently reported that Flo, a popular period tracking app, had been sharing user data with Facebook, informing the social media giant of every log in, and every time a user told the app she intended to get pregnant. The data had unique identifiers, meaning it could be matched to a device or a profile. This in turn means that Facebook could match the dates and target individuals with specific ads. (Flo has since clarified that it never had the intention to share any data.)

The problem isn't limited to easily downloadable apps. There's a large amount of ignorance of what details Indians give out on wearable devices, too, says Gupta. The lack of awareness, he feels, also stems from the lack of legal protection that would obligate a service provider to spell out its terms and put up a full disclosure.

At least till the time an enforceable law comes in, it's left to people to decide where one's data is being shared. But "the real harm of putting out data is that once it is out, the individual can't take back control of it," says Kodali.

'THERE ARE MAJOR ISSUES AND MINOR ONES, LIKE FORGETTING YOUR CHILD'S VACCINATION CHARTS.THIS MADE US REALISE THE NECESSITY OF DIGITISING HEALTH RECORDS'

SOHIT KAPOOR & HARSH PARIKH
Founders, DRiefcase