HSA ADVOCATES
HEMANT SAHAI ASSOCIATES

LAW & POLICY UPDATE

CORPORATE & COMMERCIAL

Security of individual's vaccination electronic data: Who is liable?

By: Saurya Bhattacharya, Partner

The vaccination drive in India has been consistently gaining scale, providing a sense of relief to our frontline workers, elderly and those with co-morbidities. A big section of those eligible have successfully scheduled their appointments after providing relevant details electronically, either through the Aarogya Setu app or the Co-Win website online. At the same time, periodically there have been reports of glitches and errors on these electronic platforms.

In this background, we look at the question of how legally secure an individual's electronically collected vaccination related data is, and who might be liable for any leak or loss of such individual's information.

Sensitive Personal Data

The Personal Data Protection Bill, 2019, waiting in the wings, has specific description of "health data" as a component of 'sensitive personal data'. However, for the time being, reliance is placed on the Information Technology Act, 2000 (**ITA**). 'Sensitive personal data or information' (**SPDI**) is generically defined under the ITA as such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit. However, that sensitive personal data has a more specific definition to include medical information is well established, and covered under the Information Technology (Reasonable Security Practices an Procedures and Sensitive Personal Data or Information) Rules, 2011 (**ITR**).

Under Rule 3 of the ITR, SPDI includes an individual's personal information relating to his physical, physiological and mental health condition as well as medical records and history. As we are aware, prior to vaccination, an individual has to provide his co-morbidities, information around pregnancy, allergies and such like. All of such information would constitute part of physical and physiological condition as well as medical records/history. In other words, not only the information of being vaccinated, but also related information furnished would constitute an individual's sensitive personal data, in terms of the ITR.

Section 43A of the ITA

The question that thus arises is how well the ITA protects the above. The well-known Section 43A not only provides the above referred generic definition of SPDI that leads us to Rule 3 of the ITR, but also deals with compensation for failure to protect personal data. Thereunder, a body corporate that:

- Possesses, deals or handles any SPDI in a computer resource that it owns, controls or operates;
- Is negligent in implementing and maintaining reasonable security practices and procedures, and
- Thereby causes wrongful loss or wrongful gain to any person;

would be liable to pay damages by way of compensation to the person so affected. The affected person, in this case, would primarily be the individual who registered for the vaccination and furnished his health and medical information. It is, however, unclear who could be held responsible. In a vaccination drive, the key implementing stakeholders are the government (both union and states); the tech service provider who is maintaining the electronic platforms whereby vaccination related information is being saved or shared between relevant stakeholders; and the vaccination centres (which, in turn could be government health centres, government hospitals, or private medical facilities).

While each of the above would have requirements around protection of an individual's medical information, most of them would typically not be structured as a body corporate. The only exception would be the tech service provider, thereby reducing the scope of checking for negligence that causes wrongful loss or wrongful gain to only a single entity. This could, reasonably, lead to an inference that in a mass scale inoculation drive by the government, the scope of Section 43A protection may often be narrow.

Electronic Health Records

Reference is made to the Electronic Health Record Standards, 2016 (**EHRS**), that the Ministry of Health and Family Welfare introduced with a view to keeping pace with the needs of having a uniform standard-based system for creation and maintenance of electronic health records by healthcare providers. In addition, the EHRS also describes who could constitute 'healthcare provider'. It would be an individual or an institution that provides preventive, curative, promotional or rehabilitative healthcare services in a systematic way to individuals, families and communities. No doubt, information and sensitive personal data furnished by an individual for the purposes of getting vaccinated would fall within the scope of what constitutes electronic health records. Commendably, the EHRS does speak about medical data being generated by a healthcare provider being held in trust for the individual, and the ownership remains with the individual itself. It does reasonably well in terms of relating the EHRS to the ITA as well. However, by its very nature, the EHRS is not a document that speaks of liability and consequences. If one connects back to the ITA for liability, it would likely lead to Section 43A referred above, with its limitations.

Healthcare Provider and Clinical Establishments

For an alternate approach, we consider the origin of the EHRS, which are in the Clinical Establishments (Central Government) Rules, 2012 (**CER**). Rule 9 of the CER lists certain conditions required for registration and continuation of clinical establishments. One such requirement is that electronic health records of patients be maintained and provided in accordance with standards determined by the Central Government. CER, in turn, is born under Clinical Establishments (Registration and Regulation) Act, 2010 (**CEA**). CEA does have penal provisions for different forms of non-compliances. However, it largely hinges on the concept of 'clinical establishment' and not 'healthcare providers.'

'Clinical establishment', in terms of Section 2(c) of the CEA, refers to:

- A hospital, maternity home, nursing home, dispensary, clinic, sanatorium or an institution by whatever name called that offers services, facilities requiring diagnosis, treatment or care for illness, injury, deformity, abnormality or pregnancy in any recognized system of medicine established and administered or maintained by any person or body of persons, whether incorporated or not; or
- A place established as an independent entity or part of an establishment referred to above, in connection with the diagnosis or treatment of diseases where pathological, bacteriological, genetic, radiological, chemical, biological investigations or other diagnostic or investigative services with the aid of laboratory or other medical equipment, are usually carried on, established and administered or maintained by any person or body of persons, whether incorporated or not.

As is evident, this definition is significantly different from that of 'healthcare provider', including the key difference that a healthcare provider's scope seems to include preventive healthcare services to communities, while a clinical establishment's does not. Notwithstanding, it can be argued that a clinical establishment in terms of the CEA that is part of the vaccination drive would also be a 'healthcare provider' for the purposes of the EHRS.

Consequences under the CEA

There are various forms of consequences under the CEA, notable among those being:

- Cancellation of registration of a clinical establishment, for non-compliance of conditions of registration (Section 32). It is anticipated that the EHRS would directly or indirectly be covered under this.
- If not, as an alternate one might refer to monetary penalties for non-compliance of the Act for which no specific penalty is prescribed (Section 40). When contextualized to sensitive personal data breach, the amounts appear relatively low, with a first offence attracting a penalty up to INR 10,000, the second an amount up to INR 50,000 and for subsequent offences, an amount up to INR 500,000.

There are penalties for minor curable offences, which might not be relevant in the context of this article. There are also penalties in relation to offences by companies and persons responsible for the same. In the present context, Section 44 of the CEA explains that 'company' would include firms and other association of individuals. There is also a curious situation of protection of government actions taken in good faith, which seems is arguably wide enough to cover such government's role as owning, controlling or managing a clinical establishment.

In other words, the CEA effectively creates a liability regime that is largely focused on private clinical establishments, excluding the governments and tech service providers.

Concluding Remarks

Breach of sensitive personal data (especially medical information) is a serious aspect, that often has social and psychological effects that go beyond financial loss to an individual. India has a track record of medical data leaks, including Covid test results of individuals in the last year. The ITA read with the CEA does go some way in covering liability for negligence. However, it appears to need more teeth, especially in case of culpability of government action.

Connect with us

 www.hsalegal.com

 mail@hsalegal.com

 HSA Advocates