KHAITAN &CO
Advocates since 1911

NEWSFLASH

ERGO
Analysing developments impacting business

COMING SOON: A DATA PRIVACY REGIME FOR THE HEALTHCARE SECTOR IN INDIA

27 April 2018

On 21 March 2018, the Ministry of Health and Family Welfare (MoHFW) placed the draft of the Digital Information Security in Healthcare Act (DISHA) in public domain for inviting comments. DISHA aims to secure the privacy and confidentiality of digital health data (DHD) in India. So far, India did not have a separate legislation governing DHD, and provisions of the Information Technology Act, 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (SPDI Rules) primarily governed any e-health data collected, stored and processed by relevant entities.

Once DISHA comes into effect, it will be mandatory for all "clinical establishments" and "Health Information Exchanges" to collect, store, use or transmit DHD strictly for the purposes prescribed under the Act, while maintaining utmost confidentiality and security in respect of such DHD. This Ergo provides a bird's eye view of the salient features of DISHA (as it appears in the present draft form).

What constitutes DHD?

DHD is defined as any electronic record of health-related information about an individual ("Owner"), and includes *inter alia* any information pertaining to:

(a) physical or mental health of an individual;

(b) any health service provided to an individual;

(c) donation of any body part or bodily substance;

(d) information derived during testing or examination of body part or bodily substance;

(e) information collected while providing health services; etc.

Which organisations will be governed by DISHA?

DISHA predominantly seeks to govern clinical establishments (which includes hospitals, maternity home, nursing home/ other entities in healthcare sector, whether private or Government owned and controlled or single doctors, and has been adopted from the Clinical Establishments (Registration and Regulation) Act, 2010) and Health Information Exchanges. Some obligations and compliances have also been imposed upon other 'entities.' The term 'Entity' has been defined under DISHA and includes body corporates outside India dealing with DHD, which makes DISHA's applicability extra-territorial. However, it must be noted that the

usage of the term is ambiguous and inconsistent, since the capitalised term has only been used in one provision.

Rights of Owner in respect of their DHD

DISHA *inter alia* empowers the Owner with several rights. In what appears to be a culmination of the Supreme Court of India's judgment declaring the 'right to privacy' as a fundamental right, the Owner is afforded the right to privacy, security and confidentiality of their DHD. They are provided with the right to refuse consent for the generation and collection of their DHD. To further empower the Owner, the term 'consent' has been defined comprehensively under DISHA and the concept of 'informed consent,' has been introduced. Consent, if given, can also be subsequently withdrawn. In line with the concept of 'data minimisation' (i.e. only adequate and necessary amounts of data should be collected), DISHA empowers the Owner by stating that collection of DHD shall be specific, relevant and not excessive in relation to the purpose for which it is sought. An Owner also has a right to have their DHD that is stored with a clinical establishment or Health Information Exchange rectified within 3 (three) working days.

Right of Owner to not be refused health services

A distinguishing feature of DISHA is that the obligation of a clinical establishment to provide health services to an individual is not made conditional on such individual consenting to generate, collect, store, transmit or disclose their DHD. In other words, the Owner cannot be refused health care if they choose not to part with their DHD.

Purposes of collection, storage, transmission and use of DHD

The purposes of collection, storage, transmission and use of the DHD have been categorically spelt out under DISHA and are exhaustive in nature. According to DISHA, DHD may be generated, collected, stored and transmitted by a clinical establishment *inter alia* to advance the delivery of medical care of the patient, to help guide medical decisions, improve public health activities, facilitate early identification of public health threats and emergencies and to carry out public health and academic research.

Notably, the access to, use or disclosure of DHD, whether identifiable or anonymized is prohibited for commercial purposes. There is also a blanket prohibition on the access to, use or disclosure of such data by insurance companies (except for processing of insurance claims with the consent of the Owner), employers, HR consultants and pharmaceutical companies and other entities as may be specified by the Government.

Obligations on Regulated Entities under DISHA

As per the draft, clinical establishments can collect DHD from the Owner only after obtaining consent, in form and manner as will be prescribed under DISHA. Further, clinical establishments need to inform the Owner of their rights, including right of refusal, purpose of collection of health data, identity of recipients to whom such data may be disclosed, and identity of recipients who may access DHD on a need to know basis. Clinical establishments will need to furnish a copy of the consent with the Owner. The draft also proposes requirements for consents from minors and individual who are incapacitated or incompetent to provide consent.

Breach Notification

As per the present draft of DISHA, a clinical establishment or Health Information Exchange is required to provide immediate notice and in no event later than 3 (three) working days to the Owner if there is any breach or serious breach of DHD. A serious breach is said to have occurred when, *inter alia*, the breach is intentional, or repeated or its security not ensured as per the standards in the DISHA or if it is used for commercial gains.

Consequences for Non-compliances

Any person or company who breaches DHD is liable to pay compensation to the Owner whose data has been breached. In case of a serious breach, a person can be punished with

imprisonment, which extends from 3 (three) years to 5 (five) years or fine, which is not less than INR 500,000.

Authorities under DISHA

DISHA also envisages the creation of a National Electronic Health Authority of India and various State Electronic Health Authorities, for *inter alia* the purpose of formulating standards, operational guidelines and protocols for dealing with DHD.

Adjudicating Authorities

DISHA envisages establishment of adjudicatory authorities at both Central and State levels. An aggrieved Owner can approach the relevant State authority by way of a complaint in case of a breach of DHD by a clinical establishment or other entity. In other words, DISHA ousts the jurisdiction of any other court or judicial authority to adjudicate upon such disputes. If a party is aggrieved by the decision of a State adjudicatory authority, they may appeal to the one at the Centre. An appeal against the order of the Central Adjudicatory Authority will lie to the High Court within 60 days from the date of communication of the decision or order.

Comment

MoHFW has attempted to draw out an exclusive and comprehensive data protection legislation in the realm of DHD by incorporating various data protection principles. This will have significant and far-reaching implications for the healthcare sector. Relevant regulated entities in healthcare sector will now have additional obligations and compliances once draft DISHA (in its current form) becomes law.

However, the draft of DISHA is plagued with certain loopholes and inconsistencies, which one hopes will be plugged during the course of the public comments. One significant concern area is the clinical establishments' obligation to provide health services even though the Owner may have refused to provide their consent for generating, using, storing or transmitting their DHD. Clinical establishments and Health Information Exchanges will remain on their toes as DISHA also requires them to conduct regular training to ensure that their personnel comply with DISHA's provisions.

Further, DISHA also seeks to govern entities other than clinical establishments and Health Information Exchanges that are seized of DHD. This inclusion significantly expands the applicability of DISHA as it may even bring organisations (including those incorporated outside India) that deal with health data of their employees as a part of dispensing insurance coverage and other welfare schemes, within its fold.

It will be interesting to see what shape the legislation will eventually take. It appears from the construct of the legislation that there would be significant aspects/portions that would be rolled out through further rules. It will be interesting to watch out for those as well. Also, the manner in which DISHA will co-exist with the forthcoming data protection legislation in India will be an intriguing prospect.

- *Harsh Walia (Associate Partner), Supratim Chakraborty (Associate Partner), Shweta Dwivedi (Principal Associate), Shobhit Chandra (Senior Associate) and Arindam Bhattacharjee (Associate)*

For any queries please contact: editors@khaitanco.com

Mumbai
One Indiabulls Centre, 13th Floor
Tower 1 841, Senapati Bapat Marg
Mumbai 400 013, India

T: +91 22 6636 5000
E: mumbai@khaitanco.com

New Delhi
Ashoka Estate, 12th Floor
24 Barakhamba Road
New Delhi 110 001, India

T: +91 11 4151 5454
E: delhi@khaitanco.com

Bengaluru
Simal, 2nd Floor
7/1, Ulsoor Road
Bengaluru 560 042, India

T: +91 80 4339 7000
E: bengaluru@khaitanco.com

Kolkata
Emerald House
1 B Old Post Office Street
Kolkata 700 001, India

T: +91 33 2248 7000
E: kolkata@khaitanco.com