Dr Milind Antani Partner and Head of Pharma, Life Science and Healthcare Practice
milind.antani@nishithdesai.com
Darren Punnen Associate
Anay Shukla Advocate
Nishith Desai Associates, Mumbai

DISHA: The first step towards securing patient health data in India

"A journey of a thousand miles begins with a single step." The Digital Information Security in Healthcare Act ('DISHA') is that firm first step taken by the Indian Government in the long journey to securing the healthcare data of patients in India. In a country with more than one billion people, data is bound to be scattered, even more so when it comes to healthcare data. It is common practice for a doctor to have to write up a repeat diagnostic test because they have no way of accessing the patient's medical records. This is despite the fact that the law requires doctors to maintain the medical records of their in-patients for at least three years. In a move to drastically improve healthcare delivery in India and protect patient data, DISHA proposes to change all of that. Dr Milind Antani, Darren Punnen and Anay Shukla of Nishith Desai Associates discuss the aims of DISHA, the positive response to the first public draft and the concerns raised that are likely to be addressed before the legislation is finalised.

'DISHA' in Hindi means 'direction' and the word was chosen with the purpose and objective of showing direction and putting the important data of patients on the right path. Almost two years in the making, DISHA has three primary objectives - setting up a central and state level digital health authority, enforcing privacy and security measures for digital health data, and regulating the storage and exchange of electronic health data. Before deep diving into each of these aspects, it is also important for readers to understand the current legal framework for data privacy in India.

The current legal framework

The collection, receipt, storage, handling and transfer of sensitive personal data or information ('SPDI') in electronic form is subject to the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules 2011 (the 'Data Protection Rules'), a set of rules prescribed under the Information Technology Act 2000 - India's principal legislation governing information technology. The Data Protection Rules consider a select set of information to be SPDI. From a healthcare perspective, this includes information relating to physical, physiological and mental health conditions, sexual orientation as well as medical records and history.

The Data Protection Rules apply to any corporate entity that in some way deals with the SPDI of a person. The compliance requirements under the Data Protection Rules were largely limited to obtaining consent prior to collection or transfer, publishing a privacy policy, and maintaining 'reasonable' security practices and procedures to protect SPDI. While there is a requirement for entities to meet ISO standards for data protection, it is also possible for them to have a user agree that their existing data protection practices, irrespective of whether they match ISO standards or not, are reasonable. This workaround would, in effect, satisfy the compliance requirements under the Data Protection Rules.

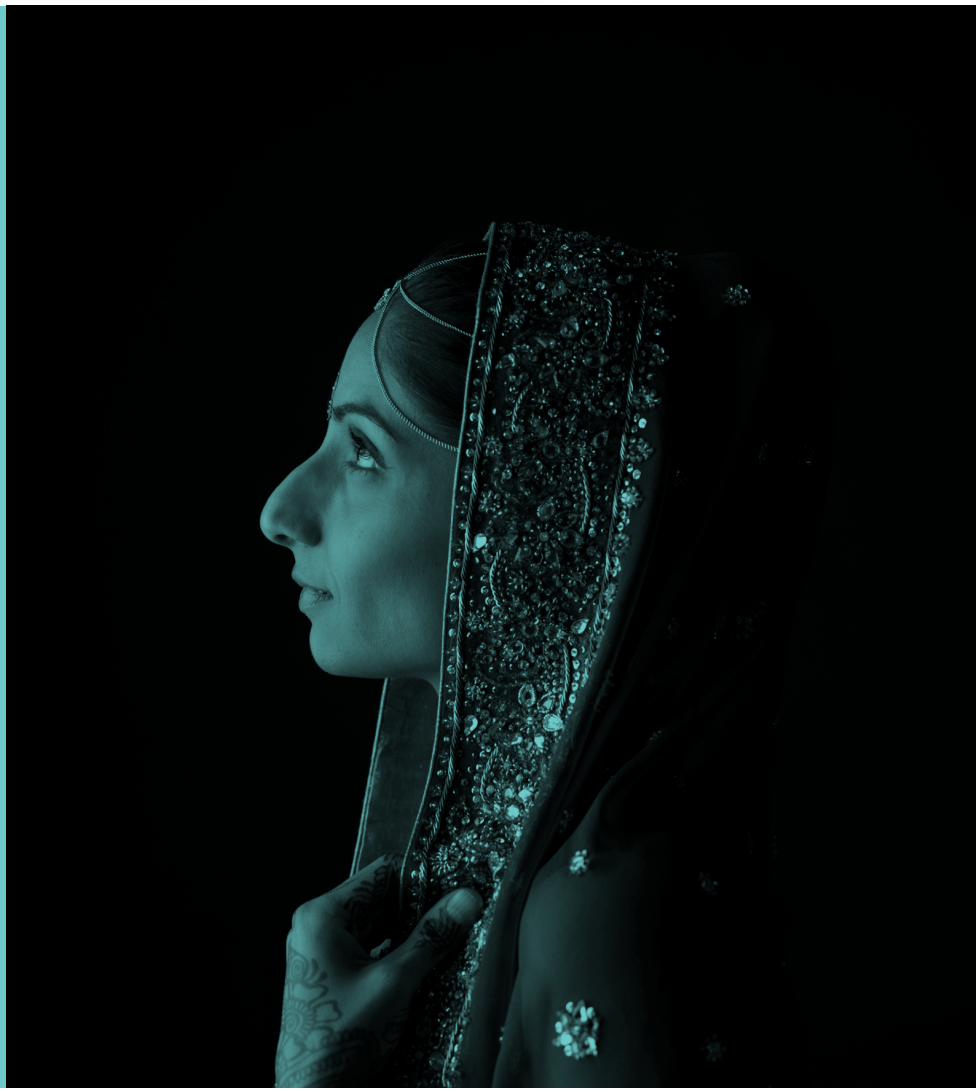
While the Data Protection Rules were a welcome step at a time when protection of electronic data was not regulated at all, the need for higher standards of protection has been felt increasingly over the years, especially when it comes to sensitive health information. The other major problem that the country has been facing is with respect to the lack of interoperability of health records between hospitals, clinics and diagnostic centres, and in extreme cases, even between two departments of the same institute. The Government did, at various instances, nudge the industry into adopting a more uniform health information system, the last attempt being in 2016 when the Government came out with a revised Electronic Health Records Standard of India. Given the non-binding nature of the recommendations, unfortunately, these efforts did not bear much fruit.

DISHA was born, therefore, out of the need to provide for better healthcare information security in a way that the public could claim as a right and to ensure interoperability of electronic health data. When finalised and introduced as law, it will replace the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules of 2011 and thereby usher India into a new regime of protection and regulation of electronic health data.

The detail of DISHA

DISHA aims to be a piece of

While the Data Protection Rules were a welcome step at a time when protection of electronic data was not regulated at all, the need for higher standards of protection has been felt increasingly over the years, especially when it comes to sensitive health information.



legislation focused on healthcare data privacy, confidentiality, security and standardisation. DISHA will create regulatory authorities, both at the central and state level, to enforce the rights and duties envisaged under the legislation. At the central level, the setting up of a National Electronic Health Authority ('NeHA') is proposed, which would be the apex authority entrusted with formulating standards and operational guidelines and protocols for the generation, collection, storage, and transfer of digital health data. At the state level, the State Electronic Health Authority ('SeHA') will be responsible for ensuring that the requirements of DISHA are followed on the ground, at the institutional level.

Clinical establishments of all kinds will be obliged to comply with the requirements of DISHA, including diagnostic centres and even individual clinics. DISHA also proposes the setting up of Health Information Exchanges - the backbone of interoperability and access - which would process and transmit data between clinical establishments. From an enforcement perspective, DISHA also establishes central and state adjudicating authorities, which will investigate complaints regarding breach of DISHA by clinical establishments and other entities, health exchanges and even NeHA and SeHA. While all citizens have a fundamental right to privacy enshrined within the Indian Constitution (the Supreme Court, in the recent case of *Justice K.S Puttaswamy (Retd.) v. Union of India and Ors*, held that the right to privacy is an intrinsic part of the right to life and personal liberty), DISHA specifically lays down the rights of the owners of health data. Informed consent and the right to know are the central themes behind the disclosure, transfer and access to digital health data. DISHA also clearly demarcates ownership of the data. While the actual digital health data is at all times owned by the individual whose health data have been digitised, the medium of storage and transmission of the digital health data is owned by the clinical establishment or the Health Information Exchange, as the case may be.

Additionally, DISHA clearly states that the digital health data of any individual is always held in trust for the owner. Individuals have the right to know exactly when digital health data is accessed or transferred as well as having the right to withdraw any consent provided, at any time. The individual also has the right to rectify mistakes in the digital health data at any time as well.

Interoperability is a crucial aspect covered by DISHA. NeHA, once established, will be required to come up with operating guidelines and standards which are to be uniformly followed by any person or entity that is involved in the generation, collection, transmission or disclosure of digital health data. Health Information Exchanges will facilitate the flow of data between entities, with the Chief Health Information Executive of each Health Information Exchange being required under DISHA to ensure the smooth day-to-day operations of the Exchange. The flow of digital health data unhindered by compatibility issues between entities would go a long way to providing better healthcare delivery for patients and improving coordination between different functions, especially in times of emergency.

While a wide set of rights are provided to owners of data, DISHA will also impose duties on collectors, generators and processors of digital health data. Maintaining privacy and confidentiality is the foremost responsibility of all stakeholders - from

continued

the clinical establishment to NeHA. DISHA also specifies the purposes for which digital health data can be collected, stored, transmitted or used by a person or entity. The owner of the data must be informed of any breach of the privacy or confidentiality of their digital health data immediately.

Breaches of digital health data and non-compliance with the requirements of DISHA will be treated very seriously under the legislation. DISHA distinguishes between a breach and a serious breach of digital health data. A breach involves a contravention of the collection or processing norms, the destruction or unauthorised modification of data, or not securing the data as required under DISHA. A serious breach, on the other hand, involves a person intentionally, fraudulently or negligently breaching digital health data, using the data for commercial purposes and breaches involving data that is not de-identified or anonymised. In case of a serious breach, the person or entity responsible for the breach may be liable to imprisonment of up to five years, and a minimum fine of INR 500,000 (approximately $7,525). In case of a breach, the owner of the data may be entitled to compensation from the person or entity responsible for the breach.

A portion of the fine payable in case of a serious breach may also be paid as compensation to the individual whose data was breached, at the discretion of the court adjudicating on the matter.

The response to the first draft

Overall, the first public draft of DISHA was received well, thanks to its clear emphasis on healthcare data privacy, protection and confidentiality, as well as the push towards interoperability. There were, however, a few issues raised that are sure to be addressed before the legislation is finalised.

A point of concern with the current version of DISHA relates to access to digital health data. The Chief Health Information Executive of a Health Information Exchange is permitted under law to access digital health data. As an Exchange that is responsible for the processing and transfer of digital health data, it may not be necessary for any person working within the Health Information Exchange to be provided with access to any of the digital health data, as the Exchange is merely an intermediary between the clinical establishment and the owner of the data. Limiting access to digital health data would go a long way to minimising the risk of an inadvertent data breach.

Similarly, all digital health data - be it from the clinical establishment or the Health Information Exchange - is held on behalf of NeHA, according to DISHA. DISHA also permits NeHA to use the information for certain limited purposes such as public health research, provided the privacy and confidentiality of the owner of the data is not compromised. While the intent of permitting NeHA to have unbridled access to the nation's digital health data is in the wider interest of trying to facilitate research and promote early detection of diseases, a breach in this situation is a matter of concern, especially considering that national databases of identifiable information have been subject to breaches in the past.

Something that remains unclear in the draft version of DISHA is the extent of interoperability envisaged for digital health data. Considering that there would be multiple Health Information Exchanges set up for the purpose of allowing interoperability, the seamlessness and interoperability between these Exchanges is something that remains to be seen.

For example, if a clinical establishment in one part of the country transferred digital health data to a Health Information Exchange, and another clinical establishment in another part of the country requested the same information, but from a different Health Information Exchange, the draft is not very clear on how digital health data would flow between exchanges. This may, however, become clear once the rules relating to DISHA are notified.

Another point that may be a major concern to industry relates to the absolute prohibition that DISHA places on access to digital health data, whether anonymised or otherwise, by pharmaceutical companies and insurance companies as well as access for any commercial purpose. This appears to be an impediment to the clinical research activities of pharmaceutical companies, as health related data is required to be submitted to the drug regulator for marketing approvals of new drugs. Given that India is currently promoting clinical research in the country, it appears that this limitation may not have been intentional, and an exception allowing pharmaceutical companies to access digital health data for this limited purpose, as well as further clarity defining the scope of commercial purposes, may find its way into the final draft of DISHA.

There also seems to be some overlap in terms of what instances of non-compliance amount to a breach or a serious breach. For instance, failure to secure data in accordance with prescribed standards is mentioned in what constitutes a breach and a serious breach under DISHA. This may be clarified or further fleshed out before the legislation is finalised. Last but not the least, it is also difficult to understand why the scope of a new piece of legislation such as DISHA, which grants important rights to citizens relating to their own healthcare data, limits those rights to healthcare data in electronic form only.

Given that DISHA has only completed its first round of comments from the public and stakeholders, it is expected that the revisions made based on the feedback will churn out a more refined version of the legislation. In any case, it is evident from the draft that the Government has really pushed to provide additional security, privacy and confidentiality for individuals, with respect to their digital health data.

A lot of thought and effort has gone into the draft - right from the clever use of the acronym DISHA to the fine distinctions made between the kinds of digital health data (de-identified and anonymised data, for example) - which is proof that when it comes to protecting privacy and confidentiality, India is definitely moving in the right 'disha.'