Chambers AND PARTNERS

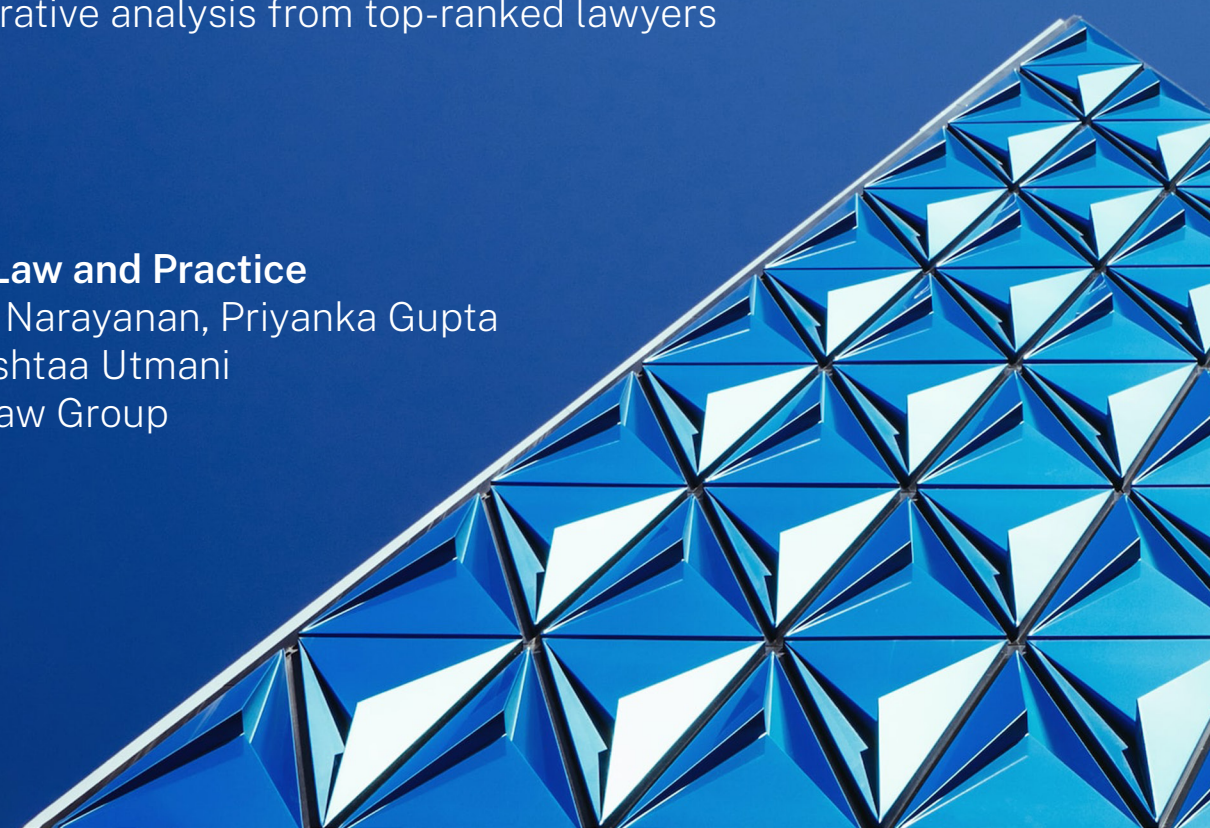
CHAMBERS GLOBAL PRACTICE GUIDES

Cybersecurity 2025

Definitive global law guides offering comparative analysis from top-ranked lawyers

India: Law and Practice

Anoop Narayanan, Priyanka Gupta and Rishtaa Utmani
ANA Law Group



INDIA

Law and Practice

Contributed by:
Anoop Narayanan, Priyanka Gupta and Rishtaa Utmani
ANA Law Group

Contents

ANA Law Group is a full-service law firm based in Mumbai, with a team of experienced professionals who have broad industry knowledge and specialisation across a wide spectrum of business areas. The firm has significant experience in counselling international clients on data privacy and cybersecurity law issues in India, and regularly represents clients from various industries. The firm works with global clients to implement privacy programmes, create compliant processes, products and services. It also assists international companies with carrying out transfer impact assessments, drafting and negotiating contracts with Indian counterparts, and preparing privacy policies for international companies operating in India and their Indian subsidiaries. The firm routinely advises clients on issues such as permitted data processing, consent requirements, data collection, retention and disclosure, regulatory requirement compliance, transfer of sensitive personal data, security breaches and drafting security breach policies, on international compliance projects, and on prosecutions and offences.

Authors

Anoop Narayanan is the founder of ANA Law Group, with vast advisory and transactional experience in all areas of Indian law. In practice for more than 30 years, Anoop is a distinguished intellectual property, TMT and employment law expert in India. He focuses on intellectual property, IT, outsourcing, employment, technology, data protection, cybersecurity, telecommunications and entertainment law matters, and his practice encompasses litigation and commercial/transactional advice. He has also advised many multinational banks on Indian data protection law, outsourcing, bank secrecy and related matters. Anoop has spoken at a number of Indian and international forums on his areas of practice and published many articles in leading national dailies and international publications.

Rishtaa Utmani is an associate in ANA Law Group's technology and IP practice group.

Priyanka Gupta is a senior attorney at ANA Law Group with more than 18 years of experience. She has strong domain knowledge and extensive experience in advising on data privacy, TMT, outsourcing, employment and intellectual property law issues. Her practice encompasses both litigation and commercial/transactional advice in these areas. Priyanka has extensive legal and practical knowledge in data privacy and cybersecurity laws in India, and advises international clients on data privacy and cybersecurity legal and regulatory issues in India. She routinely advises on issues such as data transfers, consent requirements, data collection, retention and disclosure requirements, employee-related privacy issues, cyber breach handling and preparing compliant programmes for clients under Indian law.

ANA Law Group

7th Floor
Keshava
Bandra Kurla Complex
Bandra East
Mumbai 400 051
India

Tel: +91 22 6112 8484
Email: mailbox@anaassociates.com
Web: www.anaassociates.com

1. General Overview of Laws and Regulators

1.1 Cybersecurity Regulation Strategy

The National Cyber Security Policy, established by the Ministry of Electronics and Information Technology (MeitY) in 2013, aims to improve the cybersecurity framework in India, leading to specific actions and programmes to enhance the security posture of India's cyberspace. The National Cyber Security Policy prescribes various objectives, which include the following:

- to create a secure cyber-ecosystem in the country, generate adequate trust and confidence in IT systems and transactions in cyberspace and thereby enhance adoption of IT in all sectors of the economy;
- to create an assurance framework for the design of security policies and for promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (product, process, technology and people);
- to strengthen the regulatory framework for ensuring a secure cyberspace ecosystem;
- to enhance and create national and sectoral level 24x7 mechanisms for obtaining strategic information regarding threats to ICT infrastructure, creating scenarios for response, resolution and crisis management through effective predictive, preventive, protective, response and recovery actions;
- to enhance the protection and resilience of the critical information infrastructure by operating a National Critical Information Infrastructure Protection Centre, and mandating security practices related to the design, acquisition, development, use and operation of information resources;
- to improve visibility of the integrity of ICT products and services by establishing infrastructure for testing and validation of security of such products;
- to enable protection of information while in process, handling, storage and transit so as to safeguard privacy of citizens' data and for reducing economic losses due to cybercrime or data theft;
- to enable effective prevention, investigation and prosecution of cybercrime and enhancement of law enforcement capabilities through appropriate legislative intervention; and

- to enhance global co-operation by promoting shared understanding and leveraging relationships for furthering the cause of security of cyberspace.

The National Cyber Security Policy also recommends strategies for creating a secure cyber ecosystem and an assurance framework, encouraging open standards, strengthening the regulatory framework, creating mechanisms for the early warning of security threats, vulnerability management and response to security threats, creating cybersecurity awareness, etc.

The government is working towards updating its National Cybersecurity Strategy in order to improve its position in cyberspace. The updated National Cybersecurity Strategy is a long-awaited policy initiative of the government and is expected to bring in stronger security standards and priority allocation once it is notified.

1.2 Cybersecurity Laws

The right to privacy (including the right to data security) of all citizens is protected as part of the right to life and personal liberty under Articles 19 and 21 of the Constitution of India, and as part of the freedoms guaranteed by Part III of the Constitution. This was also upheld by the Supreme Court of India (SCI) in 2017 in its landmark judgment of Justice K S Puttaswamy (Retd) and Another v Union of India and Others (2017) 10 SCC 1.

The Indian government enacted India's first comprehensive legislation on data protection in August 2023 – ie, the Digital Personal Data Protection Act, 2023 (DPDPA), with the intent to provide a legislative framework for data protection and privacy. However, the DPDPA has not as yet been implemented and enforced. The Indian government also released the draft Digital Personal Data Protection Rules, 2025 (the *"Draft DPDP Rules"*) in January 2025, for stakeholder comments. The Draft DPDP Rules seek to operationalise the DPDPA and create a solid implementation framework for protection of digital personal data. The Draft DPDP Rules will be set in place after public consultation.

At present, the Information Technology Act, 2000 (ITA) and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (the *"SPDI Rules"*) are the primary legislation for governing cybersecurity, data breach notification and incident response in India.

The ITA defines *"cybersecurity"* as *"protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorised access, use, disclosure, disruption, modification or destruction"*. The ITA empowers the central government to authorise any government agency to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource, to enhance cybersecurity, and to prevent data breaches.

Further, the SPDI Rules prescribe protection of personal information and sensitive personal data (SPD) and reasonable security practices and procedures to be implemented for collection and the processing of personal information or SPD. The SPDI Rules define personal information as *"any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person"*. The SPDI Rules recognise the following as SPD:

- password;

- financial information, such as bank account, credit card or debit card, or other payment instrument details;
- physical, physiological and mental health condition;
- sexual orientation;
- medical records and history;
- biometric information;
- any detail relating to the above as provided to a body corporate for providing service; and
- any of the information received from a body corporate in respect of the above, for processing, stored or processed under lawful contract or otherwise.

However, once the DPDPA is enforced, it will repeal the SPDI Rules.

The government has established the Indian Computer Emergency Response Team (the *"CERT-In"*) for performing various functions related to cybersecurity in India, including responding to cybersecurity incidents and implementing measures to reduce the risk of cybersecurity incidents.

The Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 (the *"CERT-In Rules"*) regulate the duties and operations of CERT-In with respect to cybersecurity incidents, such as incident response and reporting, prediction, prevention and analysis of cybersecurity incidents.

The CERT-In Rules mandate CERT-In to operate an Incident Response Help Desk on a 24-hour basis, including government and other public holidays. Earlier, the service providers, intermediaries, data centres and body corporates handling SPD had to mandatorily report all cybersecurity incidents to CERT-In *"as early as possible"*. In April 2022, CERT-In issued a new directive which modified obligations under the CERT-In Rules, including requirements to report cybersecurity incidents within six hours, syncing system clocks to the time provided by government servers, maintaining security logs in India, and storing additional customer information. CERT-In has also set up sectoral Computer Emergency Response Teams to implement cybersecurity measures at a sectoral level. The details regarding the methods and formats for reporting cybersecurity accidents, vulnerability reporting and remediation, incident response procedures and dissemination of information on cybersecurity are published on CERT-In's website and are updated from time to time.

The ITA prescribes that any service provider, intermediary, data centre, body corporate or person who fails to provide the information called for by CERT-In or comply with CERT-In's directions will be punished with imprisonment for a term which may extend to one year or a fine which may extend to INR100,000 or both.

The ITA also prescribes deterrence in terms of compensations, penalties and punishments for offences such as damage to computer systems, failure to protect data, computer-related offences, theft of computer resource or device, SPD leak, identity theft, cheating by impersonation, violation of privacy, cyberterrorism, online pornography (including child pornography), breach of confidentiality and privacy, and breach of contract.

For critical sectors, the government has set up the National Critical Information Infrastructure Protection Centre (NCIIPC) under the ITA, as the nodal agency, and has framed rules and guidelines to protect the nation's critical information infrastructure (CII) from unauthorised access, modification, use, disclosure and disruption to

ensure a safe, secure and resilient critical information infrastructure in the country.

Other relevant rules framed under the ITA for regulating cybersecurity are as follows:

- The Information Technology (Information Security Practices and Procedures for Protected System) Rules, 2018, prescribe security measures for protected systems, as defined under the ITA. Under the ITA, the government may notify any computer resource that affects the facility of CII to be *"protected system"*.
- The Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021 require intermediaries to implement reasonable security practices and procedures to secure their computer resources and information, maintaining safe harbour protections. Intermediaries are also mandated to report cybersecurity incidents to CERT-In.

Indian criminal laws contain cybersecurity-related provisions, specifically punishment for criminal offences including those committed in cyberspace. The Indian criminal laws have recently undergone regulatory changes in line with the new age technologies. In particular, the Indian Penal Code, 1860, was replaced by the *Bhartiya Nyaya Sanhita*, 2023, (BNS), the Code of Criminal Procedure, 1973, was replaced by the *Bhartiya Nagarik Suraksha Sanhita*, 2023, (BNSS) and the Indian Evidence Act, 1872, was replaced by *Bhartiya Sakshya Adhiniyam*, 2023, (BSA), with effect from July 2024. Under the BNS, continued cyber-crimes and economic offences are referred to as *"organised crime"*. The BSA specifies that electronic records will be considered as primary records, which calls for a strong foundation to be laid to protect the data online. The BNS criminalises the forging of false electronic documents and imposes a punishment of seven years' imprisonment and a fine.

Additionally, the Companies (Management & Administration) Rules, 2014 formulated under the Companies Act 2013, require companies to implement security systems to ensure that electronic records are secured from unauthorised access.

1.3 Cybersecurity Regulators

The Cyber Law Division, operating under MeitY, assumes a pivotal role in implementing cybersecurity measures.

Under the ITA, the Indian government has established CERT-In as the national nodal agency for cybersecurity, to carry out the following functions:

- collection, analysis and dissemination of information on cyber incidents;
- forecast and alerts of cybersecurity incidents;
- emergency measures for handling cybersecurity incidents;
- co-ordination of cyber incidents response activities;
- issue of guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, response and reporting of cyber incidents; and
- such other functions relating to cybersecurity as may be prescribed.

The CERT-In Rules prescribe that CERT-In will be responsible for responding to cybersecurity incidents and will assist cyber-users in the country in implementing measures to reduce the risk of cybersecurity incidents. CERT-In also has powers to issue directions to service providers, intermediaries, data centres, body corporates,

etc, for enhancing cybersecurity infrastructure in the country.

The NCIIPC is the nodal agency for the protection of CII, networks and systems in the country.

In addition to MeitY and NCIIPC, the government has established the National Security Council Secretariat (NSCS) as the central co-ordinating body for cybersecurity and internet governance. NSCS has developed a draft cybersecurity strategy to address the issue of security of national cyberspace, with the main aim being to improve the audit quality relating to cybersecurity to aid the organisations in conducting a better review of their cybersecurity knowledge and architecture. Currently, there is no implementation date for this strategy.

The Ministry of Home Affairs (MHA) has set up the Cyber and Information Security Division (C&IS) to deal with matters relating to cybersecurity, cybercrime, the National Information Security Policy & Guidelines and its implementation. C&IS is comprised of a cybercrime wing, a cybersecurity wing, an information security wing and a monitoring unit.

Further, the MHA has established the Indian Cybercrime Co-ordination Centre (I4C), which is a nodal point in the fight against cybercrime, and provides a platform to deal with cybercrimes in a coordinated and comprehensive manner, while coordinating the implementation of mutual legal assistance treaties with other countries. The I4C has launched the Citizen Financial Cyber Fraud Reporting and Management System in several Indian states, to facilitate the immediate reporting of financial fraud and prevent fund siphoning by fraudsters.

The government has also set up the National Technical Research Organisation (NTRO) as a technical intelligence agency under the National Security Advisor in the Prime Minister's office. NTRO's primary role is to develop technology capabilities in aviation and remote sensing, data gathering and processing, cybersecurity, strategic hardware and strategic monitoring. The NCIIPC falls within NTRO's ambit.

The ITA mandates the central government to appoint an adjudicating officer to conduct inquiries, and adjudicate matters (ie, contravention of any of the provisions of the ITA or any rule, regulation, direction or order made thereunder, including non-compliance with CERT-In's direction), with claims for injury or damages valued up to INR50 million. Claims that exceed this amount must be filed before the competent civil court. Where more than one adjudicating officer is appointed, the ITA mandates the central government to specify the matters and places of jurisdiction of each adjudicating officer.

The inquiry and investigation procedure for the adjudicating officer is provided under the Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules, 2003. Any decision of the adjudicating officer can be appealed before the Telecom Disputes Settlement and Appellate Tribunal (TDSAT).

Under the DPDPA, the Central Government has the power to establish the Data Protection Board of India (DPB). The DPB is the primary regulatory body responsible for enforcing the DPDPA legislation. Data principals are required to comply with applicable laws while exercising their rights under the Act. Breach of the duties by data principals may result in penalties of up to INR10,000. The maximum penalty for violation

of the DPDPA's provisions by a data fiduciary is INR2.5 billion, for failure to take reasonable security safeguards to prevent a personal data breach if the non-compliance is regarded as significant by the DPB.

The DPDPA also prescribes specific penalties of INR2 billion for failure to notify the DPB and affected data principals of data breaches, and non-compliance with additional obligations while processing children's data.

Under the DPDPA, the TDSAT established under the Telecom Regulatory Authority of India Act, 1997 adjudicates on appeals from the orders of the DPB, and the SCI is the final appellate authority for all purposes under the DPDPA.

The following non-governmental authorities assist the Indian government in cybersecurity measures:

- the Data Security Council of India (DSCI) – a not-for-profit industry body under the National Association of Software and Services Companies (NASSCOM) that engages with governments and their agencies, regulators, industry sectors, industry associations and think tanks for policy advocacy, thought leadership, capacity-building and outreach activities;
- National Cyber Safety and Security Standards (NCSSS) – a self-governing body to protect the CII from cyber-related issues;
- the Internet and Mobile Association of India (IAMAI) – a not-for-profit industry body that addresses the issues, concerns and challenges of the Internet and mobile economy;
- the Cellular Operators Association of India (COAI) – an industry association of mobile service providers, telecoms equipment, internet and broadband service providers in India, which interacts directly with ministries, policymakers, regulators, financial institutions and technical bodies;
- the Internet Service Providers Association of India (ISPAI) – the recognised apex body of Indian ISPs worldwide; and
- the Computer Society of India (CSI) – a non-governmental organisation of professionals (software developers, scientists, academics, project managers, etc) who contribute to the government's formulation of information technology strategy and planning.

Sector-Specific Regulators

Additionally, there are various sector-specific regulators engaged in supervising their relevant intermediaries on the progress of implementation and robustness of cybersecurity frameworks. They regularly conduct cybersecurity and system audits of the intermediaries, which are reported to the relevant regulators.

Banking sector

The Reserve Bank of India (RBI) governs both public and private sector banks. The RBI's guidelines prescribe that the RBI can request an inspection at any time of any of the banks' cyber-resilience. The RBI has set up a Cyber Security and Information Technology Examination (CSITE) cell under the Department of Banking Supervision, to periodically assess the progress made by banks in the implementation of the cybersecurity framework, and other regulatory instructions and advisories through on-site examinations and off-site submissions. The RBI has an internal ombudsman scheme for commercial banks with more than ten branches as a redressal forum, and has also issued guidelines on information security, electronic banking, technology risk management and cyber fraud. CERT-In and the RBI jointly carry out a cybersecurity awareness campaign on *"Beware and*

be aware of financial frauds" through the Digital India Platform.

RBI also issued Guidelines on Regulation of Payment Aggregators and Payment Gateways, directing payment aggregators to put in place adequate information, data security infrastructure and systems for prevention and detection of fraud, and has specifically recommended implementation of data security standards and best practices such as PCI-DSS, PA-DSS, the latest encryption standards and transport channel security. Payment aggregators must establish a mechanism for monitoring, handling and follow-up of cybersecurity incidents and breaches, and mandatorily report incidents to RBI and CERT-In.

RBI regularly conducts audits and inquiries into banks' security frameworks and imposes penalties on the banks for non-compliance with RBI's cybersecurity framework. RBI has also formulated an integrated scheme, The Reserve Bank – Integrated Ombudsman Scheme, 2021 to simplify the grievance redressal process at RBI by enabling the customers of all regulated entities to register their complaints at one centralised reference point. Through this portal, RBI also spreads cyber-crime awareness including frauds using mobile apps/UPI/QR codes, etc.

Insurance sector

The Insurance Regulatory and Development Authority (IRDA) is the nodal agency for governance and regulation of the insurance sector in India. The IRDA conducts regular on-site and off-site inspections of insurers to ensure compliance with the legal and regulatory framework. The IRDA also has issued guidelines on Information and Cyber Security for Insurers (IRDA Cyber Security Policy), which requires vulnerability assessment and penetration testing annually and closing any identified gaps within a month. Some other relevant guidelines issued by IRDA are: IRDAI (Outsourcing of Activities by Indian Insurers) Regulations, 2017; IRDAI (Maintenance of Insurance Records) Regulations, 2015; and the IRDAI (Protection of Policyholders' Interests) Regulations, 2017, which contain a number of provisions and regulations on data security. Additionally, IRDA has issued guidelines to insurers on structuring cyber-insurance for individuals and identifying gaps that need to be filled. As per the guidelines, cyber-insurance should provide cover against theft of funds and identity, unauthorised online transactions, email spoofing, etc.

Telecoms sector

Telecoms operators in India are governed by regulations laid down by the following regulatory bodies:

- the Telecom Regulatory Authority of India (TRAI);
- the Department of Telecom (DoT);
- the TDSAT;
- the Group on Telecom and IT (GOTIT);
- the Wireless Planning Commission (WPC); and
- the Digital Communications Commission (DCC).

Further, the Unified Access Service Licence (UASL) extends information security to the telecom networks as well as to third-party operators. The regulator requires telecom operators to audit their network (internal/external) at least once a year.

TRAI has released its recommendations on cloud services in relation to creation of a regulatory framework for cloud services, and constituting an industry-led body of all cloud service providers (CSP).

In August 2024, the DoT released the Telecommunications (Telecom Cyber Security) Rules, 2024, which place obligations on telecommunications entities to take measures to ensure telecoms cybersecurity. These measures obligate the entity to adopt a telecoms cybersecurity policy, to identify and reduce the risks of security incidents, ensure timely responses to such incidents, take appropriate action for addressing security incidents, and mitigate their impact, etc.

The DoT also released the Telecommunications (Critical Telecommunication Infrastructure) Rules, 2024, which authorise the Union Government to declare any telecommunications network or part thereof as Critical Telecommunication Infrastructure, disruption of which will severely impact national security, economy, public health or safety.

The DoT regularly conducts cybersecurity workshops and cyber drills for better awareness.

Securities sector

The Securities Exchange Board of India (SEBI) was established in 1988 and is the regulatory body for commodity and security markets in India. SEBI oversees the interests of investors and market intermediaries, and ensures that the issuers of securities are protected, including safeguarding their customer data, data and transactions. In April 2022, SEBI appointed six committee members to advise regarding the cybersecurity initiatives for the Indian economy and guide SEBI to maintain and develop cybersecurity requirements keeping in mind the global industry standards.

In August 2024, SEBI issued a Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities.

2. Critical Infrastructure Cybersecurity

2.1 Scope of Critical Infrastructure Cybersecurity Regulation

The ITA empowers the government to identify critical information infrastructure and prescribe the information security practices and procedures for protected systems.

- Critical Information Infrastructure (CII): The ITA defines *"Critical Information Infrastructure"* as *"the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety"*.
- Protected System: Any computer resource which directly or indirectly affects the facility of CII, may be notified by the government as *"Protected System"* under the ITA.

For critical sectors, the government has set up the NCIIPC under the ITA, as the nodal agency for the protection of the CII, networks and systems in India. Critical sectors include but are not limited to energy, finance, banking, telecommunications, transportation and defence.

The NCIIPC has framed the Information Technology (Information Security Practices and Procedures for Protected System) Rules, 2018 (the *"NCIIPC Rules"*) and issued Guidelines for the Protection of National Critical Information Infrastructure, 2015, (*"NCIIPC Guidelines"*) to protect India's CII from unauthorised access, modification, use, disclosure and disruption to ensure a safe, secure and resilient information infrastructure for critical sectors in the country.

The NCIIPC Guidelines prescribe that each critical sector is responsible for the identification and categorisation of CIIs within their infra-

structures on the basis of functionality, criticality scale, degree of complementarities political, economic, social and strategic values, degree of dependence, sensitivity, etc.

In the financial sector, the government has declared the following along with their associated infrastructures to be *"Protected Systems"*:

- the Real Time Gross Settlement (RTGS);
- the National Electronic Funds Transfer (NEFT);
- e-Kuber (Core Banking Solution) of the Reserve Bank of India;
- computer resources relating to the Unified Payments Interface, Immediate Payment Service and National Financial Switch, being CII of the National Payments Corporation of India; and
- various computer resources relating to the CII of several banks in India such as Union Bank of India, State Bank of India, ICICI Bank, HDFC Bank, Canara Bank, Axis Bank, to name a few.

The NCIIPC regularly advises on reducing vulnerabilities of the CII, and against cyberterrorism, cyberwarfare, and other threats. The NCIIPC Guidelines prescribe the development of audit and certification agencies for the protection of the CII. The NCIIPC also exchanges cyber incidents and other information relating to attacks and vulnerabilities with CERT-In and concerned cybersecurity organisations in India.

2.2 Critical Infrastructure Cybersecurity Requirements

The CERT-In Rules require all cybersecurity incidents to be reported, including attacks on critical infrastructure and compromise of critical systems/information.

The NCIIPC Rules lay down the cybersecurity practices and procedures to be followed in respect of CII and protected systems. The NCIIPC Rules prescribe that all organisations having *"Protected System"* shall constitute an Information Security Steering Committee under the chairmanship of the Chief Executive Officer/Managing Director/Secretary of the organisation.

The organisations having *"Protected System"* are required to undertake the following responsibilities:

- nominate an officer as Chief Information Security Officer (CISO) with roles and responsibilities as per latest NCIIPC Guidelines and *"Roles and Responsibilities of CISOs of Critical Sectors in India"* released by NCIIPC;
- plan, establish, implement, operate, monitor, review, maintain and continually improve Information Security Management System (ISMS) of the *"Protected System"* as per latest NCIIPC Guidelines or an industry accepted standard duly approved by the NCIIPC;
- ensure that the network architecture of *"Protected System"* and any changes shall be documented. Further, the organisation shall ensure that the *"Protected System"* is stable, resilient and scalable as per latest NCIIPC Guidelines;
- plan, develop, maintain, review the documentation of authorised personnel having access to *"Protected System"* as well as the documents of inventory of hardware and software related to *"Protected System"*;
- ensure that Vulnerability/Threat/Risk (V/T/R) Analysis for the cyber security architecture of *"Protected System"* shall be carried out at least once a year. Further, Vulnerability/Threat/Risk (V/T/R) Analysis shall be initiated whenever there is significant change or

upgrade in the system, under intimation to ISSC;
- plan, establish, implement, operate, monitor, review, and continually improve Cyber Crisis Management Plan (CCMP) in close co-ordination with NCIIPC;
- ensure conduct of internal and external Information Security audits periodically;
- plan, develop, maintain and review documented process for IT Security Service Level Agreements (SLAs), which shall be strictly followed while designing the SLAs with service providers;
- establish a Cyber Security Operation Centre (CSOC) using tools and technologies to implement preventive, detective and corrective controls to secure against advanced and emerging cyber threats. In addition, CSOC is to be utilised for identifying unauthorised access, unusual and malicious activities on the *"Protected System"*, by analysing the logs on regular basis. The records of unauthorised access, unusual and malicious activity, if any, shall be documented;
- establish a Network Operation Center (NOC) using tools and techniques to manage control and monitor the network(s) of the *"Protected System"* for ensuring continuous network availability and performance; and
- plan, develop, maintain and review the process of taking regular backup of logs of networking devices, perimeter devices, communication devices, servers, systems and services supporting the *"Protected System"* and the logs shall be handled as per the ISMS.

The CISO is required to maintain regular contact with the NCIIPC and is responsible for implementing the security measures suggested by NCIIPC using all available/appropriate ways of communication.

The CISO is mandated to share the following, whenever there is any change, or as required by the NCIIPC, and incorporate the inputs/feedbacks suggested by the NCIIPC:

- details of CII declared as the *"Protected System"*, including dependencies on and of the said CII;
- details of Information Security Steering Committee (ISSC) of the *"Protected System"*;
- Information Security Management System (ISMS) of the *"Protected System"*;
- network architecture of the *"Protected System"*;
- authorised personnel having access to the *"Protected System"*;
- inventory of hardware and software related to the *"Protected System"*;
- details of Vulnerability/Threat/Risk (V/T/R) Analysis for the cyber security architecture of the *"Protected System"*;
- Cyber Crisis Management Plan (CCMP);
- Information Security Audit Reports and post Audit Compliance Reports of the *"Protected System"*; and
- IT Security Service Level Agreements (SLAs) of the *"Protected System"*.

The NCIIPC Rules require the CISO to establish a process, in consultation with the NCIIPC, for sharing of logs of the *"Protected System"* with the NCIIPC to help detect anomalies and generate threat intelligence on a real-time basis. The CISO must also establish a process of sharing documented records of the CSOC (related to unauthorised access, unusual and malicious activity) of the *"Protected System"* with the NCIIPC to facilitate issue of guidelines, advisories and vulnerability, audit notes, etc, relating to the *"Protected System"*. The CISO is also required to establish a process for timely communication

of cyber incidents on the *"Protected System"* to the NCIIPC.

Additionally, CERT-In is mandated to exchange relevant information relating to attacks, vulnerabilities and solutions in respect of critical sectors with NCIIPC.

Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of the ITA shall be punished with imprisonment which may extend to ten years and a fine.

2.3 Incident Response and Notification Obligations

As per the CERT-In directive of 2022, certain types of cybersecurity incidents are to be mandatorily reported by service providers, intermediaries, data centres, body corporate and government organisations to CERT-In, within six hours of noticing such incidents or being brought to notice about such incidents. These cybersecurity incidents include, inter alia:

- targeted scanning/probing of critical networks/systems;
- compromise of critical systems/information; and
- attacks on critical infrastructure, SCADA and operational technology systems and wireless networks.

The NCIIPC Guidelines also recommend that cybersecurity breach incidents must be reported to the NCIIPC.

The NCIIPC's latest Standard Operating Procedure (SOP) on Incident Response shall be strictly followed in case of cybersecurity incidents impacting the national CII. Based on NCIIPC's latest SOP on Incident Response (2017), in case of any security incident, the victim organisation should operate as follows.

- Report the same to NCIIPC as early as possible.
- Nominate a suitable official and convey their contact information to NCIIPC. This individual must be able to provide technical details related to the incident, and/or must be able to make the required technical personnel available.
- Arrange a meeting with the OEM/System Integrator.
- Provide all relevant logs to NCIIPC through secure FTP hosted by NCIIPC. Log files need to be password protected and the password should be communicated through any media other than the internet.
- Obtain the necessary in-house administrative approvals and clearance for a visit from the Incident Response Team to the incident site or data centre facility.

2.4 State Responsibilities and Obligations

The National Cyber Security Policy 2013, lays down the protection and resilience of CII, building a secure and resilient cyberspace, and creating mechanisms for security threat early-warning, vulnerability management, and response to security threats as some of the primary responsibilities of the government.

The policy envisages that large-scale cyber incidents may overwhelm the government, public and private sector resources and services by disrupting the functioning of critical information systems. Some examples of cyber threats to individuals, businesses and government are identity theft, phishing, social engineering, hactivism, cyber terrorism, compound threats targeting mobile devices and smart phones,

compromised digital certificates, advanced persistent threats, denial of service, bot nets, supply chain attacks, data leakage, etc.

The policy prescribes that the government should work towards rapid identification, information exchange, investigation and co-ordinated response and remediation, which can effectively mitigate the damage caused by malicious cyberspace activity.

CERT-In is the main authority responsible for analysing trends and patterns in intruder activities, determining the scope, priority and threat of a cyber incident and developing preventive strategies against cybersecurity incidents. With the aim of identifying cybersecurity vulnerabilities and promoting resilience, CERT-In follows *"Responsible Vulnerability Disclosure and Coordination Policy"*, wherein it collects, analyses, and mitigates co-ordination with researchers/finders and vendors leading to the public disclosure of newly identified cybersecurity vulnerabilities and threats.

Upon receiving any information regarding a cybersecurity vulnerability, CERT-In will examine and validate the vulnerability report and communicate to the discloser whether or not the report will be co-ordinated by CERT-In. Upon successful validation, CERT-In will initiate co-ordination with the relevant product vendor, discloser and other stakeholders (if required) for the remediation and closure of the issue. CERT-In will endeavour to get the issue resolved within 120 days from initial vendor contact date.

CERT-In publishes the vulnerability note/advisory on its website after the vulnerability is addressed or at an appropriate time determined by CERT-In in synchronisation with the stakeholder.

Additionally, the NSCS has released Cyber Security Audit – Baseline Requirements (CSA-BR) prescribing minimum, common and harmonised baseline requirements for cybersecurity audits, which are to be mandatorily followed by all CII. These guidelines are applicable to regulators and owners of CII and entail the following stages – management, protection, detection, response, recovery and lessons learnt.

3. Financial Sector Operational Resilience Regulation

3.1 Scope of Financial Sector Operational Resilience Regulation

India does not have a comprehensive financial sector operational resilience regulation under the current cybersecurity framework.

However, with the aim of improving the cybersecurity framework in India's financial sector, in August 2024, the SEBI released the Cybersecurity and Cyber Resilience Framework (CSCRF), for SEBI Regulated Entities (the *"Regulated Entities/RE"*) which includes, inter alia, the following:

- alternative investment funds (AIFs);
- bankers to an issue (BTI) and self-certified syndicate banks (SCSBs);
- clearing corporations;
- collective investment schemes (CIS);
- credit rating agencies (CRAs);
- custodians;
- debenture trustees (DTs);
- depositories and depository participants;
- investment advisers and research analysts;
- KYC registration agencies; and
- merchant bankers.

The CSCRF defines *"cyber-resiliency"* as *"the ability of an organisation to continue to carry out*

its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing, and rapidly recovering from cyber incidents".

The CSCRF is standards-based and broadly aligns with the cyber-resiliency goals of CERT-In's Cyber Crisis Management Plan for countering cyberattacks and cyber terrorism. These goals include: anticipating, withstanding, containing, recovering, and evolving in response to threats, in addition to the core cybersecurity objectives of identifying, detecting, protecting, responding, and recovering. The CSCRF framework provides a structured methodology to implement various solutions for cybersecurity and cyber resiliency. The CSCRF framework supersedes earlier SEBI circulars and guidelines.

The RBI also released a Guidance Note on Operational Risk Management and Operational Resilience in April 2024 (*"Guidance Note"*) which applies to Regulated Entities (*"REs"*) including all commercial banks, primary (Urban) Co-operative Banks/State Co-operative Banks/Central Co-operative Banks, All-India Financial Institutions and All Non-Banking Financial Companies including Housing Finance Companies.

RBI's Guidance Note intends to promote and further improve the effectiveness of Operational Risk Management of the REs, and enhance their Operational Resilience in view of the interconnections and interdependencies, within the financial system, that result from the complex and dynamic environment in which the REs operate.

3.2 ICT Service Provider Contractual Requirements

There is no specific definition or provisions dealing with *"ICT service providers"* under the current cybersecurity law framework in India.

However, RBI's Guidance Note mentions that third-party service providers, inter alia, include cloud service providers and IT/operations vendors. The Guidance Note prescribes that REs should perform a risk assessment and due diligence before entering into arrangements with such third-party service providers. Particularly, the RE should verify whether the third-party service provider has at least an equivalent level of operational resilience to safeguard the RE's critical operations in normal circumstances, and in the event of a disruption.

Further, the Guidance Note recommends that a policy approved by the board of directors on the management of service providers is critical for managing risks associated with reliance on third parties irrespective of whether they are related or unrelated to the RE. Such third-party risk policies should include:

- procedures for determining whether there is a need for entering into a third-party arrangement for a service and how to enter into such an arrangement;
- sound structuring of the third-party arrangement, including ownership and confidentiality of data, as well as termination rights;
- programmes for managing and monitoring the risks associated with the third-party arrangement, including the financial condition of the service provider;
- establishment of an effective control environment at the RE and the service provider that should include a register of third-party relationships (that identifies the criticality of

different services) and metrics and reporting to facilitate oversight of the service provider; and
- execution of comprehensive contracts and/or service level agreements (which are enforceable) with a clear allocation of responsibilities between the third-party service provider and the RE, provided the ultimate responsibility vests with the RE.

REs, in their agreements with the third-party service providers, should also include clauses making the service provider contractually liable for the performance and risk management practices of its sub-contractors.

As per the CSCRF, REs are required to identify and classify critical systems based on their sensitivity and criticality for business operations, services and data management. The board/partners/proprietor of the RE shall approve the list of critical systems. The CSCRF does not specify whether ICT services or cloud service providers will be considered as critical systems.

3.3 Key Operational Resilience Obligations

The key objective of the CSCRF is to address evolving cyber threats, to align with the industry standards, to encourage efficient audits, and to ensure compliance by SEBI REs. The CSCRF also sets out standard formats for reporting by REs.

The CSCRF lays down that REs are required to establish, communicate and enforce cybersecurity risk management roles, responsibilities and authorities to foster accountability and continuous improvement. A comprehensive cybersecurity and cyber-resilience policy shall be documented and implemented with the approval of the board/partners/proprietor.

CSCRF mandates Market Infrastructure Institutions (MIIs), Qualified REs and mid-size REs to prepare a cyber risk management framework for identification and analysis, evaluation, prioritisation, response and monitoring of cyber risks on a continuous basis. MIIs and Qualified REs must also prepare a Cyber Capability Index (CCI). MIIs shall conduct third-party assessment of their cyber-resilience using CCI on a half-yearly basis. Qualified REs shall perform self-assessment of their cyber-resilience using CCI on a yearly basis.

Risk assessment (including post-quantum risks) of RE's IT environment also must be done on a periodic basis. REs shall establish appropriate security mechanisms through a Security Operations Centre for continuous monitoring of security events and timely detection of anomalous activities.

REs shall be solely accountable for all aspects related to third-party services including (but not limited to) confidentiality, integrity, availability, non-repudiation, security of their data and logs, and ensuring compliance with laws, regulations, circulars, etc, issued by SEBI/Indian government. Accordingly, REs shall be responsible and accountable for any violations of the same.

Incident and Reporting Obligations

As per the CSCRF, the REs are required to establish a comprehensive Incident Response Management plan and corresponding SOPs, as well as formulate an up-to-date Cyber Crisis Management Plan. In the event of an incident, Root Cause Analysis (RCA) shall be conducted to identify the cause leading to the incident.

Under the CSCRF, cyber-attacks, cybersecurity incidents and breaches experienced by REs falling under CERT-In's 2022 directive, must be notified to SEBI and CERT-In within six hours

of noticing/detecting such incidents or being brought to notice about such incidents. This information also has to be shared to the SEBI Incident Reporting Portal within 24 hours.

Stock brokers/depository participants shall also report the incident to stock exchanges/depositories as well as SEBI and CERT-In within six hours of noticing/detecting such incidents or being brought to notice about such incidents. Any/all other cybersecurity incidents shall be reported to SEBI, CERT-In, and NCIIPC (as applicable) within 24 hours.

During the life cycle of incident handling, some aspects must be captured, such as whether the RE has followed its organisation's incident response plan, taken necessary (immediate) measures to contain the incident impact and to control, mitigate and remediate the incident, whether the RE has communicated about the incident to all relevant stakeholders, etc.

The RE shall undertake the necessary activities and submit the relevant reports within timelines prescribed in the CSCRF. Thereafter, SEBI shall examine the incident on the basis of reports submitted. Further, the RE shall classify the cybersecurity incident based on its severity and the same shall be reviewed and submitted to SEBI.

In case an RE does not report a cybersecurity incident to SEBI (despite being aware of the incident) in the prescribed manner, SEBI may take appropriate regulatory action depending on the nature of the incident.

Additionally, as per RBI's Guidance Note, REs should maintain an inventory of incident response and recovery, internal and third-party resources to support its response and recovery capabilities. The scope of incident management should capture the life cycle of an incident, typically including, but not limited to:

- the classification of an incident's severity based on predefined criteria (eg, expected time to return to business as usual), enabling proper prioritisation and assignment of resources to respond to an incident; and
- the incident response and recovery procedures, including their connection to the RE's business continuity, disaster recovery and other associated management plans and procedures.

Incident response and recovery procedures should be periodically reviewed, tested and updated by the REs. They should also identify and address the root causes of incidents to prevent or minimise serial recurrence.

3.4 Operational Resilience Enforcement

There are no specific operation resilience enforcement obligations or provisions for critical ICT service providers under the current cybersecurity regime.

3.5 International Data Transfers

The DPDPA permits the transfer of personal data for the purpose of processing to any country or territory outside of India, except to such territories which may be restricted by the government via notification. However, the DPDPA has not as yet been implemented and enforced.

As per the SPDI Rules which are currently in force, the transfer of sensitive personal data or information to a third-party company/individual outside of India is permitted if the recipient ensures the same level of data protection that is adhered to by the transferor. Further, the personal data may only be transferred based on the consent of the relevant company/individual or

for the performance of a contract with the company/individual.

3.6 Threat-Led Penetration Testing

The CSCRF for REs prescribes that Vulnerability Assessment and Penetration Testing (VAPT) must be done to detect vulnerabilities in the IT environment for all critical systems, infrastructure components, and other IT systems as defined in the framework.

CSCRF specifies a comprehensive scope for VAPT. The scope of the IT environment taken for the VAPT should be made transparent to SEBI and should include all critical assets and infrastructure components including (not limited to) networking systems, security devices, servers, databases, applications, systems accessible through WAN, LAN as well as with public IPs, websites, etc.

Testing Methodology

The VAPT should provide in-depth evaluation of the security posture of the system through simulations of actual attacks on its systems and networks. The testing methodology should be adapted from the following:

- SEBI CSCRF;
- NCIIPC;
- CERT-In Rules;
- The National Institute of Standards and Technology Special Publication 800-115;
- Latest ISO27001;
- PCI-DSS standards;
- Open Source Security Testing Methodology Manual; and
- OWASP Testing Guide.

As regards the insurance sector, the IRDA also has a cybersecurity policy requiring vulnerability assessment and penetration testing annually and closing any identified high-risk gaps within a month. The RBI also mandates banks to have periodical vulnerability assessment and penetration testing exercises for all critical systems.

Further, the DPDPA requires significant fiduciaries to undertake measures including data protection impact assessment and periodic audits. The *"Data Protection Impact Assessment"* is defined as a process comprising description, purpose, assessment of harm, measures for managing the risk of harm and such other matters concerning the processing of personal data, as may be prescribed.

4. Cyber-Resilience

4.1 Cyber-Resilience Legislation

While India's National Cyber Security Policy states *"building a secure and resilient cyberspace"* as one of its primary objectives, at present there is no specific legislation governing cyber-resilience in India under the current cybersecurity regime.

However, there are sector-specific frameworks for cyber-resilience, such as the CSCRF for SEBI's REs, which is outlined in **3. Financial Sector Operational Resilience Regulation**.

4.2 Key Obligations Under Legislation

Please refer to **4.1 Cyber-Resilience Legislation**.

5. Security Certification for ICT Products, Services and Processes

5.1 Key Cybersecurity Certification Legislation

The current Indian law does not include cybersecurity certification legislation.

With regards to CII organisations, the NCIIPC Guidelines prescribe security certifications by third-party agencies (government or private agencies) to protect the assets of a CII for smooth and error-free operation. The certifications must also deal with enforcing or implementing any international security standards available globally for the protection of critical assets working in the CII by respective organisations. Each CII must list the certifications needed to be implemented for the protection of their assets and the areas involved.

In addition to the certification of the CII facility, the CII must also ensure that the personnel hold certifications relevant to their responsibilities and up to date with the current standards. Accordingly, knowledge upgradation programs via new certifications, trainings, seminars, workshops etc. should also be planned for the employees based on the requirements of the CIIs. The implementation process of the security certifications should also be properly monitored by the CII management, so that it does not interfere with the normal functioning of the CII.

6. Cybersecurity in Other Regulations

6.1 Cybersecurity and Data Protection

Under the DPDPA, a data fiduciary is mandated to protect the personal data in its possession or under its control by taking reasonable security safeguards to prevent personal data breach. The Draft DPDP Rules also prescribe that the data fiduciary shall protect personal data by taking reasonable security safeguards to prevent personal data breach, which shall include the following:

- appropriate data security measures, including securing of such personal data through its encryption, obfuscation or masking or the use of virtual tokens mapped to that personal data;
- appropriate measures to control access to the computer resources used by such data fiduciary or a data processor;
- visibility on the accessing of such personal data, through appropriate logs, monitoring and review, for enabling detection of unauthorised access, its investigation and remediation to prevent recurrence;
- reasonable measures for continued processing in the event of confidentiality, integrity or availability of such personal data being compromised as a result of destruction or loss of access to personal data or otherwise, including by way of data backups;
- enabling the detection of unauthorised access, its investigation, remediation to prevent recurrence and continued processing in the event of such a compromise, retain such logs and personal data for a period of one year, unless compliance with any law for the time being in force requires otherwise;
- appropriate provision in the contract entered into between such data fiduciary and a data processor for taking reasonable security safeguards; and
- appropriate technical and organisational measures to ensure effective observance of security safeguards.

As per the DPDPA, the processing of personal data can only happen by way of consent of the data principal. A notice must be provided to the data principal before seeking consent. The notice should contain details about the personal data to be collected, the purpose of processing, as well as how the data principal may withdraw its consent, use the grievance redressal mechanism, and make a complaint to the DPB.

The DPDPA prescribes that the consent obtained from the data principal must be free, specific, informed, unconditional and unambiguous with clear affirmative action, and shall signify an agreement to the processing of the subject's personal data for the specified purpose and be limited to such personal data as is necessary for such specified purpose.

Consent need not be sought for legitimate uses which include processing for:

- specified purposes for which the data principal has voluntarily shared personal information without objecting to such processing;
- purposes of employment;
- responding to medical emergencies;
- performing any function under law or the state providing any service or benefit to the data principal;
- compliance with any judgment or order issued under any law; and
- taking measures to ensure safety during breakdown of public order, etc.

The Draft DPDP Rules propose that in case of personal data breaches, the data fiduciary must report the personal data breach to the DPB within 72 hours of becoming aware of such breach. If such personal data breach is in connection with a cybersecurity incident, the same must be reported to CERT-In as well as the relevant sectoral regulator, within their respective prescribed timelines.

The SPDI Rules prescribe the protection of personal information and sensitive personal data and reasonable security practices and procedures to be implemented for collection and the processing of personal information or SPD. The SPDI Rules require all body corporates to implement reasonable security practices and standards, as well as to document their security programmes and policies.

Once the DPDPA is brought into force, it will repeal the SPDI Rules.

6.2 Cybersecurity and AI

AI is not specifically dealt with under the current cybersecurity regime in India.

MeitY constituted four committees to promote AI initiatives and to develop a policy framework around it. The committees have submitted their reports on platforms and data on AI; leveraging AI for identifying national missions in key sectors; mapping technological capabilities; key policy enablers required across sectors; and on cybersecurity, safety, legal and ethical issues.

Further, MeitY, CERT-In and SISA (a global leader in forensics-driven cyber security), in September 2024, jointly launched the Certified Security Professional for Artificial Intelligence (CSPAI) program which is the first-of-its-kind ANAB-accredited AI security certification. The CSPAI program equips security professionals with the skills needed to effectively integrate AI into business applications while adhering to sustainable practices.

6.3 Cybersecurity in the Healthcare Sector

The Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002, (IMCR) impose patient confidentiality obligations on medical practitioners.

The Ministry of Health and Family Welfare introduced a draft legislation in 2017, known as the Digital Information Security in Healthcare Act (the *"DISH Act"*), to regulate the generation, collection, storage, transmission, access and use of all digital health data. The DISH Act also provides for the establishment of a National Digital Health Authority as the statutory body to enforce privacy and security measures for health data, and to regulate storage and exchange of health records.

The Ministry of Health and Family Welfare had approved a Health Data Management Policy (the *"HDM Policy"*) largely based on the DPDPA to govern data in the National Digital Health Ecosystem. The HDM Policy recognises entities such as data fiduciaries and data processors similar to the DPDPA, and establishes a consent-based data-sharing framework.

Under the DPDPA, health data can be processed by the data fiduciary as legitimate use, in case there is a medical emergency that involves a threat to life or an immediate threat to the health of a data principal or any other person or if there is a situation like an epidemic, an outbreak of a disease, or any other threat to public health.

The SPDI Rules also recognise and protect SPD which includes a person's physical, physiological and mental health condition, sexual orientation, medical records and history, and biometric information.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Rob.Thomson@chambers.com