COMPLIANCE WITH CYBERSECURITY AND PRIVACY LAWS IN THE HEALTHCARE SECTOR IN SINGAPORE

HARLEEN SETHI*

I. INTRODUCTION

Healthcare is a highly regulated industry, even in the cybersecurity and privacy law domain. Applicable laws, rules and regulations in this sector require routine risk assessments. The information pertaining to the healthcare data of patients which is collected and processed by healthcare authorities should adhere to compliance mechanisms and standards as laid down by regulatory authorities. It is essential for such data controllers and intermediaries to demonstrate compliance with such laws to mitigate the risks at hand.

II. LAWS, RULES AND REGULATIONS TO BE CONSIDERED BY THE HEALTHCARE AUTHORITIES IN ADDRESSING CYBERSECURITY, PRIVACY/DATA PROTECTION ISSUES

1. Singapore Computer Misuse Act[1]

This is the main piece of legislation in Singapore that overlooks criminal activities that take place in the online environment. Section 3 of the *CMA* establishes the principle offence under the Act, that is the "Unauthorised access" offence[2] and section 4 of the *CMA* is an aggravated computer hacking

* LLM (IP and Technology Laws) (NUS), Class of 2020.

[1] (Cap 50A, 2007 Rev Ed) [*CMA*].

[2] *CMA*, *supra* note 1, s 3(1) states that "any person who knowingly causes a computer to perform any function for the purpose of securing access without authority to any program or data held in any computer shall be guilty of an offence".

offence.[3] Sections 5, 6, 7, 8 of the *CMA* further regulate offences like unauthorised modification, unauthorised obstruction, unauthorised disclosure of access codes. The important point to note here is that in 2017, a new set of provisions were enacted under the *CMA* to criminalise activities associated with the use of personal information obtained in the breach of the other provisions under the *CMA*. Section 8A deals with the issue of identity theft in Singapore.[4] Another essential provision to note is Section 9 of the *CMA* which was adopted from the US Computer Fraud and Abuse Act[5] and introduced the concept of "protected computers". Section 9(2)(d) of the *CMA* means to include "the protection of public safety including systems related to essential emergency services such as police, civil defence and medical services" under the ambit of the definition of "protected computers".[6]

2. Singapore Cybersecurity Act[7]

The *Cybersecurity Act* is an omnibus piece of legislation which applies to all type of information and computer systems. In Singapore, which is known to be a smart city and technologically advanced in its operations, private corporations and government verticals rely heavily on the internet for provision and delivery of a wide range of services, including essential services as specified under the First Schedule of the *Cybersecurity Act*[8]. This increase in the reliance on the technological and digital network

---

[3] *Ibid*, s 4(1) states that "Any person who causes a computer to perform any function for the purpose of securing access to any program or data held in any computer with intent to commit an offence to which this section applies shall be guilty of an offence."

[4] *Ibid*; s 8A(1) provides that "A person shall be guilty of an offence if the person, knowing or having reason to believe that any personal information about another person (being an individual) was obtained by an act done in contravention of section 3, 4, 5 or 6… ."

[5] 18 U.S.C. § 1030.

[6] *CMA*, *supra* note 1, s 9(2)(d).

[7] Cybersecurity Act 2018 (Act 9 of 2018) [*Cybersecurity Act*].

[8] *Cybersecurity Act*, *supra* note 7, s 2(1) defines "essential service as any service essential to the national security, defence, foreign relations, economy, public health, public safety or public order of Singapore, and specified in the First Schedule".

stimulated environment has its pros but at the same time also exacerbates vulnerability to cybersecurity attacks which result in disruptions to such essential services, causing not only moral and economic damage, but also personal harm and loss of life. In this regard, the Cybersecurity Agency [CSA] which was set up in 2015 oversees and coordinates all aspects of cybersecurity for Singapore, ensuring cybersecurity strategy and crisis management across all critical information infrastructure [CII] sectors[9] (**which includes healthcare**). The *Cybersecurity Act* imposes duties on CII owners to ensure cybersecurity of their respective CIIs and advocates the creation of a framework for sharing cybersecurity information with CSA and for complying with the provisions of the *Cybersecurity Act*. Under the *Cybersecurity Act*, there are certain obligations which need to be complied with by CII owners. A brief summary of the same is provided below in order to highlight the important provisions which need to be taken into consideration by the healthcare sector:

(a) Section 10[10] states that the identified owner/operator of the CII has to furnish specific information; even if such information is confidential and commercially sensitive,[11] pertaining to the CII infrastructure including its set up, design, security, operation, configuration.

(b) Section 11[12] gives authority and enables the Commissioner of the CSA to regulate by prescribing standards of performance and codes of practice to the CII owners. These may not be binding in nature but have to be complied with as non-compliance attracts criminal penalties.[13] The Personal Data Protection Act 2012[14] has issued advisory guidelines on key concepts which set out factors to assess the reasonableness of security arrangements.[15]

---

[9] *Ibid*; s 2(1) defines CII as "critical information infrastructure means a computer or a computer system in respect of which a designation under section 7(1) is in effect".

[10] *Ibid*; s 10.

[11] Cybersecurity (Critical Information Infrastructure) Regulations 2018, s 4(2)(a).

[12] *Ibid*; s 11 establishes the Codes of practice and standards of performance.

[13] *Ibid*; s 12 establishes the power of Commissioner to issue written directions in the event of non-compliance.

[14] Personal Data Protection Act 2012 (No. 26 of 2012) [*PDPA*].

[15] Personal Data Protection Commission Singapore, "Advisory Guidelines on Key Concepts in the Personal Data Protection Act (revised 9 October 2019)", online: PDPC <https://www.pdpc.gov.sg/-

(c) Section 13 imposes an obligation on the CII owner to report to the CSA Commissioner any legal or beneficial change in the ownership/share of ownership in the CII.[16]

(d) Section 14(1)-(3) impose obligations on the CII owners in respect of the reporting of a cybersecurity incident within a prescribed period.[17] For this purpose, it is pertinent that the CII owners have in place a mechanism for detecting such cybersecurity threats and incidents.[18] It is for these reasons that hospitals need to put a risk management and compliance framework in place which facilitates the timely detection of such cybersecurity risks and threats, as non-compliance to these sections attracts criminal penalties.[19]

(e) Section 15[20] and section 16[21] impose additional obligations on the CII owners to conduct regular cybersecurity audits and risk assessments of their CII infrastructure by a third party approved auditor.

/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts/Advisory-Guidelines-on-Key-Concepts-in-the-PDPA-9-Oct-2019.pdf> [*PDPC Guidelines*].

[16] *Cybersecurity Act*, *supra* note 7, s 13.

[17] *Ibid*; s 14(1) states "the owner of a critical information infrastructure must notify the Commissioner of the occurrence of any of the following in the prescribed form and manner, within the prescribed period after becoming aware of such occurrence".

[18] *Ibid*; s 14(2) states "the owner of a critical information infrastructure must establish such mechanisms and processes for the purposes of detecting cybersecurity threats and incidents in respect of the critical information infrastructure, as set out in any applicable code of practice".

[19] *Ibid*; s 14(3) states "any owner of a critical information infrastructure who, without reasonable excuse, fails to comply with subsection (1) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $100,000 or to imprisonment for a term not exceeding 2 years or to both".

[20] *Ibid*; s 15(1) "The owner of a critical information infrastructure must:

(a)at least once every 2 years (or at such higher frequency as may be directed by the Commissioner in any particular case), starting from the date of the notice issued under section 7, cause an audit of the compliance of the critical information infrastructure with this Act and the applicable codes of practice and standards of performance, to be carried out by an auditor approved or appointed by the Commissioner; and

(b)at least once a year, starting from the date of the notice issued under section 7, conduct a cybersecurity risk assessment of the critical information infrastructure in the prescribed form and manner".

[21] Ibid; s 16 states "the Commissioner may conduct cybersecurity exercises for the purpose of testing the state of readiness of owners of different critical information infrastructure in responding to significant cybersecurity incidents".

In addition to this an audit or risk assessment may be ordered by the Commissioner in certain circumstances of non-compliance, misleading/inaccurate/incomplete provision of information by the CII[22] or where such assessments have not been carried out satisfactorily.[23]

III. PRIVACY AND PERSONAL DATA PROTECTION OBLIGATIONS

Singapore follows a hybrid approach with its *PDPA* as it is an extensive privacy legislation supplemented by certain sector-specific legislation.[24] The *PDPA* constitutes a comprehensive set of provisions that provides for baseline standards and requirements for the protection of personal information. All private organisations are subject to the data protection obligations under the *PDPA*.[25] The statutory definition of "personal data"[26] is stated under section 2(1) of the *PDPA*. The purpose of the *PDPA* as per Section 3 is to govern the collection, use and disclosure of personal data by organisations in a manner that balances the interests between the right of individuals to protect their personal data and the requirement of the organisation to collect, use and disclose personal data for purposes a reasonable person would consider appropriate in the business circumstances.[27] It is pertinent to note that hospitals possess a fair amount of personal information pertaining to the identification and healthcare of their patients. This information is highly sensitive in nature and as per

---

[22] *Ibid*; s 15(4).

[23] *Ibid*; s 15(5).

[24] Examples of certain sector-specific privacy legislation in Singapore: Banking Act (Cap 19, 2008 Rev Ed); Protection from Harassment Act (Cap 256A, 2015 Rev Ed); Infectious Diseases Act (Cap 137, Rev Ed 2003).

[25] Warren B Chik and Pang Keep Ying Joey, "The Meaning and Scope of Personal Data under the Singapore Personal Data Protection Act" (2014) 26 SAcLJ 354.

[26] Personal Data under the PDPA is defined as "data, whether true or not, about an individual who can be identified from that data; or from that data and other information to which the organisation has or is likely to have access".

[27] *PDPC Guidelines, supra* note 15, 31.

the *Cybersecurity Act*, comes under the ambit of CII sector.[28] Section 11 of the *PDPA* imposes and enforces that it is the primary duty of the organisation to comply with the *PDPA*.[29] It is important to note here that it is because of the sensitive and highly critical nature of the information in the healthcare sector that Singapore has proposed a Healthcare Services Bill in 2018, following the Singhealth data breach incident (as discussed below).[30] Further, sections 24[31] and 25[32] of the PDPA highlight steps to be taken by the organisation for the protection and retention of personal data.

IV. IMPACT OF SUCH RULES AND REGULATIONS IN THE HEALTHCARE SECTOR

[28] *Cybersecurity Act*, *supra* note 7, s 7(1) interprets Critical Information Infrastructure [CII] sectors to refer to such sectors that are responsible for the continuous delivery of essential services in Singapore and healthcare is one of the sectors under CII.

[29] *PDPA*, *supra* note 14, s 11(1) states that the organisation must be the one to consider whether their practices are what a reasonable person would consider appropriate under the circumstances and s 11(2) states that an organisation is responsible for personal data in its possession or under its control.

[30] Public Consultation on the Draft Healthcare Services (HCS) Bill, *Ministry of Health* (5 January 2018- 15 February 2018) online: Reach <https://www.reach.gov.sg/participate/public-consultation/ministry-of-health/corporate-communications/public-consultation-on-the-draft-healthcare-services-bill>.

[31] *PDPA*, *supra* note 14, s 24.

[32] *Ibid*, s 25.

The PDPC issued advisory guidelines for the healthcare sector in 2014, which were revisited and revised in 2017.[33] These guidelines and the *PDPA* endorse a set of basic principles[34] which governs the rules, laws and legislations under this domain that should be complied with by organisation in the process of collection, use and dissemination of personal information. These principles are also enforced by international rules and regulations, for instance the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data[35], the EU GDPR[36], Health Insurance Portability and Accountability Act [HIPAA] Privacy Rule[37] and HIPAA Security Rule[38].

The *PDPA* and the *PDPC Healthcare Guidelines*[39] provide rules and guidelines to be followed by healthcare institutions which engage third parties like data intermediaries to process personal data and also impose obligations on such institutions to oversee data processing.[40] In these unprecedented times of COVID-19, where countries around the world including Singapore are launching apps for contact tracing of affected individuals in order to flatten the curve, these rules and regulations will play an

---

[33] Personal Data Protection Commission Singapore, "Advisory Guidelines for the Healthcare Sector (revised 28 March 2017)", online: PDPC <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Sector-Specific-Advisory/advisoryguidelinesforthehealthcaresector28mar2017.pdf> [*PDPC Healthcare Guidelines*].

[34] *PDPC Healthcare Guidelines*, *supra* note 33; These basic principles include consent, use, retention, collection, transfer and purpose limitations; notification, access, security, accountability, correction, data quality, accuracy, transfer and openness obligations to be complied with by the organisations with such personal information of individuals.

[35] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2013 Rev Ed), online: OECD <https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf>.

[36] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

[37] United States Department of Health and Human Services OCR Privacy brief, "Summary of the HIPAA Privacy Rule", online: HHS <https://www.hhs.gov/sites/default/files/privacysummary.pdf>.

[38] United States Department of Health and Human Services OCR Privacy brief, "Security 101 for Covered Entities", online: HHS <https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/security101.pdf>.

[39] *PDPC Healthcare Guidelines*, *supra* note 33, 15.

[40] *PDPA*, *supra* note 14, s 4(3) states "the organisation that engages the data intermediary would still have the same obligations under the PDPA in respect of personal data processed on its behalf as if the personal data were processed by the organisation itself".

extensive role in ensuring that privacy is maintained. A repeat of the Singhealth breach would not be desirable at the moment. Given that the contact tracing app "TraceTogether" works by exchanging short distance Bluetooth signals between phones to detect other participating app users in close proximity, privacy risks are certainly elevated.[41]

A recent pertinent shift can be seen in the minds of the law and policy makers towards taking steps to strengthen legislation governing cybersecurity, privacy and data protection laws. It is submitted that the reasons for such shift can be attributed to the increase in technological advancements, the growing importance of the nature of personal information, and the absence of robust laws, rules and regulations to deal with such pertinent issues. In light of these circumstances, it is not just sufficient to execute the laws and rules in this area, but to effectively comply with and practice the same within the realities and limits of sound business practices. In view of the above, the healthcare sector needs to shift towards a proportionate compliance and risk management approach in cybersecurity, privacy and data protection laws in order to successfully maintain privacy standards and safeguard themselves from increased security and data privacy concerns.

One of the worst breaches of personal data in Singapore's history took place when between May 2015-July 2018, the personal information of 1.5 million patients and records of outpatient dispensed medicines for 160,000 of those patients were stolen, malicious accessed and copied. This information included national registration identity card numbers, gender of patients, date of birth, age which is regarded as personal information under the PDPA. This cyberattack was effected on the Singapore Health Services Pte Ltd [SingHealth] patient database system.[42]

---

[41] Dean Koh, "Singapore government launches new app for contact tracing to combat spread of COVID-19" *Mobi Health News* (20 March 2020), online: Mobi Health News <https://www.mobihealthnews.com/news/asia-pacific/singapore-government-launches-new-app-contact-tracing-combat-spread-covid-19> [*Mobi Health News*].

[42] PDPC Commissioner, "Singapore Health Services Pte. Ltd. & Ors' [2019] SGPDPC 3", online: PDPC <https://www.singaporelawwatch.sg/Portals/0/Docs/Judgments/2019/[2019]%20SGPDPC%203.pdf> [*PDPC Singhealth*].

As reiterated above, the health sector handles one of the most critical and sensitive sets of personal information. The patients have a right to expect and ensure security and protection of such data provided to the hospitals and the government in confidentiality.[43] The role of the government in collecting and processing the information pertaining to the medical history and travel whereabouts, *inter alia*, in the wake of this pandemic so as to better trace and facilitate contact tracing to identify the affected individuals and confirmed cases of COVID-19, is also to be taken into account. In view of these practices, which are no doubt critical in COVID-19 times, it is pertinent to be aware of the potential cybersecurity and privacy threats which need to be guarded against.

Once we are at a stage of flattening the curve and even whilst collecting such personal information 'privacy by design' plays an extremely essential role right through the process of inflow to the outflow of such data. Data organisations and intermediaries should prepare a checklist of the obligations to be complied with under the *Cybersecurity Act* and the *PDPA* with regard to the privacy and security of such data in order to set up a compliance framework in place to ensure all these rules, laws and regulations are complied with.

Due diligence tests need to be conducted on the third-party vendors, especially data intermediaries (specifically in cases of contact tracing via apps) which need to be engaged in order to ensure that the data intermediaries also comply with the obligations set forth on them under the *PDPA* and *PDPC Guidelines*. The data organisations should also ensure that their policies, controls and standard operating procedures are implemented and updated to log the physical/electronic movement of records and maintain an audit trail of record transactions to ensure protected safe keeping and secured access to such records.

V. CONCLUDING REMARKS

[43] *PDPC Singhealth, supra* note 42, 17.

As the SingHealth data breach case has cautioned, it is not only important to have policies and procedures in place, it is equally significant to timely and efficiently execute such procedures. The TraceTogether app which has been developed by the Government Technology Agency of Singapore in collaboration with the Ministry of Health does not collect or use location data.[44] It also does not have access to the contacts in the user's phone. It primarily uses Bluetooth data to establish a contact and all such data which is collected is stored locally on the user's phone and is encrypted.[45] It is only when an individual is confirmed to have contracted COVID-19 that the government will request the user to upload the data to the government in order to facilitate contact tracing of close contacts.[46] An additional privacy practice which is followed by the app pertains to the storage of such data wherein if a user does not come into close contact with a confirmed COVID-19 case, data which is older than 21 days will be automatically deleted.[47] It is also essential to note here that in order to flatten the curve, artificial intelligence in health care may be able to supplement manual contact tracing but cannot replace the same. It cannot pick up on nuances like false positives and negatives, which health care workers can do.[48] The apps do not account for instances beyond the algorithm activated, for instance certain factors beyond proximity like environment and activity. There are lives at stake and false positives and negatives may actually result in life and death consequences. This is why technology should be used as an aid to the human-fronted process in combating this pandemic, rather than a replacement, whilst maintaining all privacy and security standards in the healthcare sector.

Note: At the time of publication, the Personal Data Protection (Amendment) Bill 2020 had not been passed.

---

[44] *Mobi Health News, supra* note 41.

[45] *Ibid.*

[46] *Ibid.*

[47] *Ibid.*

[48] Alfred Ng, "Tech isn't the solution to COVID-19" *CNet Health and Wellness* (13 April 2020), online: CNet <https://www.cnet.com/health/director-behind-singapores-contact-tracing-app-says-tech-isnt-the-solution-to-covid-19/>.