Cybersecurity Protection for Private Practice

A LEGAL PERSPECTIVE

Text by Tham Hsu Hsien and Leong Yi-Ming

Hsu Hsien advises on medical malpractice litigation, disciplinary proceedings and healthcare regulatory matters. He is a faculty member of the SMA Centre for Medical Ethics and Professionalism and is an appointed member of the Ministry of Health's National Transplant Ethics Panel of Laypersons. He contributed towards the Singapore chapter of The International Comparative Legal Guide to Drug & Medical Device Litigation 2024.

Yi-Ming focuses on complex commercial disputes with a particular specialisation in cross-border, intellectual property and technology disputes in her practice. She previously represented Singapore Health Services in the data breach inquiry investigations and the Personal Data Protection Commission. Her broad experience covers company and shareholder disputes, equity and trusts, cryptocurrency, regulatory breaches and corporate governance.

In December 2023, the Ministry of Health (MOH) launched a public consultation on the proposed Health Information Bill (HIB). The HIB will make it mandatory for all licensed healthcare providers, including private medical practices, to contribute data into the National Electronic Health Record (NEHR), and it will also provide them with access to patients' summary medical records in the NEHR. This should improve healthcare delivery for patients, but the increased connectivity also increases the risk of cyberattacks, which healthcare is vulnerable to.

In 2018, an unprecedented and sophisticated cyberattack on the patient database of Singapore Health Services' (SingHealth) cluster of institutions resulted in some 1.5 million patient personal particulars being illegally accessed and a further subset of 159,000 patient medication records being exfiltrated over the course of a week. The then Prime Minister's personal and outpatient medication data was specifically targeted and repeatedly accessed. The Committee of Inquiry which had been convened to inquire into the events and contributing factors reported key findings on cybersecurity awareness, resources, incident responses, and weaknesses in the network and software solutions. SingHealth and its information technology administrator, Integrated Health Information Systems (now known as Synapxe), were fined S$250,000 and S$750,0000, respectively, by the Personal Data Protection Commission (PDPC) for failing to make reasonable security arrangements to prevent unauthorised access and use of the patient data in breach of the Personal Data Protection Act 2012 (PDPA).[1]

More than five years on, cybersecurity and cyber hygiene for private practices are even more important today. Patient information, history and medical data, collectively referred to as patient data, are increasingly stored and used electronically across various medical and technological solutions and devices. At the same time, the cyber threat landscape has developed significantly. More sophisticated malware have been created to infiltrate and access a victim's network, take over administrative privileges, and exfiltrate sensitive information. Cybercriminal groups use malware to extract data and extort victims by threatening the release of data unless a ransom is paid (otherwise known as ransomware attacks). Further, cyber attackers have harnessed artificial intelligence (AI) to create more advanced means of attacking through AI-driven social engineering and phishing attacks. In 2023, some 4,100 phishing attempts were reported to the Singapore Cyber Emergency Response Team.[2]

Data breaches involving patient data are serious events which may not only impact patient care, but also put patients at risk of targeted fraud, ransom and scam attacks from threat actors. Ransomware attacks may even

expose patients to injury through denial of healthcare. There are also business continuity and reputational concerns that doctors and private practices may face. It is therefore timely that the HIB should legislate a unified set of cybersecurity and data security requirements for healthcare providers, including private practices, contributing to and accessing NEHR. In preparation, MOH has published the Cyber and Data Security Guidelines for Healthcare Providers (Healthcare Cybersecurity Guidelines) in December 2023, in consultation with the Cyber Security Agency of Singapore (CSA), Infocomm Media Development Authority, and PDPC, to provide guidance and recommendations on cyber and data security aspects for the proper storage, access, use and sharing of health information, in the lead up to the implementation of the HIB.[3]

This article discusses some key considerations for private practices concerning cybersecurity protection and their legal implications.

Sources of potential responsibility for cybersecurity breaches

As a starting point, doctors and practices already have pre-existing responsibilities to secure confidential medical records and to meet their standard of care. While these may not be specifically framed in cybersecurity terms, they should broadly apply in connection with cybersecurity attacks. Among other laws, a doctor could be held responsible for professional misconduct for breach of medical confidentiality under Section C7 of the Singapore Medical Council's Ethical Code and Ethical Guidelines 2016. The medical practice could also be prosecuted for contravening Section 27 of the Healthcare Services Act 2020 for failing to (i) implement safeguards to protect medical records from accidental or unlawful loss, modification or destruction, and unauthorised access, disclosure, copying or modification; (ii) monitor or periodically evaluate the safeguards to ensure that they are effective and complied with by employees or authorised persons; or (iii) take all appropriate steps to ensure employees or authorised persons are aware of the safeguards and their role in maintaining the safeguards.

Doctors and private practices may also be exposed to civil litigation from patients for breach of a duty of confidence. If there were ransomware attacks that resulted in denial of healthcare and injury to a patient, it is conceivable that there could be a civil claim by the patient as well. In addition, as patient data includes "personal data" as described in Section 2 of the PDPA, private practices have legal obligations under the PDPA as well.

Therefore, the HIB and the Healthcare Cybersecurity Guidelines may be seen as augmenting the existing framework by which patient interests are being protected specifically from cybersecurity risks in a digital healthcare world.

Securing patient data with reasonable security arrangements

With regard to unauthorised access, misuse and exfiltration of patient data in cybersecurity incidents, pursuant to Section 24 of the PDPA, a private practice must "protect personal data in its possession or under its control by making reasonable security arrangements to prevent (a) unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks; and (b) the loss of any storage medium or device on which personal data is stored".

As previously observed by the PDPC in the SingHealth case, the reasonableness of the security arrangements adopted, in the context of medical data being personal data of a sensitive nature, would be assessed at a **higher standard of protection**.

In addition to the Healthcare Cybersecurity Guidelines, the PDPC, CSA and the Singapore Police Force (SPF) have published various guidelines and advisories to educate and inform businesses about the latest cybersecurity risks and trends, and to recommend protective and preventive measures for businesses to mitigate such risks. Some non-exhaustive examples which are potentially applicable to handling patient data from these guidelines and advisories include:

(a) Cybersecurity toolkits developed for enterprise leaders and small and medium enterprise (SME) owners.[4] The toolkits highlight the need for businesses to establish a cybersecurity workplan which includes identifying systems and information that are essential for the business, protecting these assets, and establishing that business-critical systems and data are backed up offline and available in the event of a cybersecurity incident. Cybersecurity should be integrated into a business continuity plan so that business operations are not disrupted in the event of an incident. In the context of patient data, it would likely be relevant for a private practice to identify systems containing patient data and assess their security, access and backups. The practice may also consider network segmentation (eg, having external and internal networks, guest and wireless networks) to minimise unauthorised access to patient data through the network.

(b) The Data Protection Essentials (DPE) framework and checklist, developed by the PDPC and CSA, provide a baseline standard of data protection for SMEs.[5] Should a data breach occur, the PDPC may consider an organisation's implementation of the DPE framework favourably in deciding an enforcement outcome.

(c) In recent decisions and guidelines, the PDPC has emphasised that stronger requirements are required for administrative accounts which have privileged access to systems that host or process sensitive or confidential personal data such as financial and health records. The PDPC has identified that the use of two- or multi-factor authentication (2FA or MFA) is a mandatory baseline standard for administrative accounts in addition to the use of a complex password.[6,7] The CSA has also advised that relying solely on passwords to secure users' online accounts may no longer be sufficient. In using 2FA or MFA, the CSA's view is that SMS-based authentication (through one-time passwords sent via SMS to a user's registered mobile

number) is less secure compared to other methods of authentication as SMS may be more susceptible to interception by threat actors.[8]

Accordingly, private practices could consider their current cybersecurity stance in the context of protecting patient data and determine if measures should be implemented or improved upon to reasonably protect the data and systems. Always use reliable vendors when developing or maintaining one's cybersecurity. The best way to prevent ransomware and other attacks from happening is to take preventive steps to protect business systems and its users. MOH has also identified available resources and funding to support private practices in improving their cybersecurity measures.[9]

Cybersecurity incident responses

Under the PDPA, a "data breach" in relation to personal data means: "(a) the unauthorised access, collection, use, disclosure, copying, modification or disposal of personal data; or (b) the loss of any storage medium or device on which personal data is stored in circumstances where the unauthorised access, collection, use, disclosure, copying, modification or disposal of the personal data is likely to occur."

In the event of a data breach, the PDPC recommends the following:[10]

(a) Contain the data breach to prevent further compromise of data and implement mitigating action(s) to minimise potential harms from the breach after an initial appraisal has been conducted to determine the extent of the breach.

(b) Assess the data breach to determine the root cause (where possible) and the effectiveness of containment action(s) taken thus far to contain the data breach. Where necessary, continuing efforts should be made to prevent further harm from the data breach.

(c) Report the data breach to the PDPC for a notifiable breach, and/or the affected individuals, if required (assessed pursuant to Sections 26A to 26E of the PDPA).

(d) Evaluate the organisation's response to the data breach and consider the actions that can be taken to prevent future data breaches. Where necessary, continuing efforts should be made to prevent further harm from the data breach.

The PDPA also includes mandatory data breach notification requirements. In the event of a data breach incident, certain prescribed classes of data loss which have been deemed to result in significant harm to the affected individuals would require mandatory notification to the PDPC and potentially the affected individuals. The prescribed classes of medical information and other non-clinical information in medical records that are subject to PDPA's mandatory notification are set out in the Personal Data Protection (Notification of Data Breaches) Regulations 2021. Examples of such information have also been provided by MOH.[11]

Apart from the PDPC, practices should also consider if further reports should be made to other agencies. For instance, ransomware attacks, phishing emails and business email compromises are suspected criminal acts which are reportable to SPF and CSA.

Investigations with the PDPC may subsequently result in:

(a) A suspension or discontinuation of the investigation, which may occur where the impact is assessed to be low or limited.

(b) A voluntary undertaking, which may be requested by the practice in the commencement or early stages of investigations. This may arise where the practice is able to demonstrate accountable policies and practices in place, and has a remediation plan.

(c) Investigations with findings, which may include findings of no breach, warning, directions, financial penalties, or directions and financial penalties. Financial penalties of up to S$1 million or 10% of the organisation's annual turnover in Singapore, whichever is higher, may be imposed.

Finally, in the event of a data breach, the practice may also be subject to additional civil litigation from patients for suffering loss or damage by the result of breaches of the PDPA, under Section 48O of the PDPA.

Conclusion

With the anticipated interconnectedness of patient data with the HIB, and increasing use of digital records, cybersecurity should be considered as integral components of private practices' businesses and for the protection of patient data. ◆

References

1. Re Singapore Health Services Pte Ltd & Ors [2019] PDPC 3.

2. Fall in Phishing, Infected Infrastructure and Website Defacement Incidents Reported to CSA in 2023, but Absolute Figures Remain High. In: Cyber Security Agency of Singapore. Available at: https://bit.ly/3YqVfUL. Accessed 16 October 2024.

3. Ministry of Health Singapore. Cyber & Data Security Guidelines for Healthcare Providers. Available at: https://bit.ly/3CJeWyp. Accessed 19 October 2024.

4. Toolkits for Enterprise Leaders and SME Owners. In: Cyber Security Agency of Singapore. Available at: https://bit.ly/4eHasXi. Accessed 16 October 2024.

5. Data Protection Essentials (DPE). In: Infocomm Media Development Authority. Available at: https://bit.ly/3Ubckzf. Accessed 16 October 2024.

6. Personal Data Protection Commission Singapore. How to Guard Against Common Types of Data Breaches. Available at: https://bit.ly/408U51g. Accessed 16 October 2024.

7. Lovebonito Singapore Pte. Ltd. [2022] SGPDPC 3.

8. Importance of Using Secure Multi-Factor Authentication Methods. In: Cyber Security Agency Singapore. Available at: https://bit.ly/4h95kwY. Accessed 16 October 2024.

9. How can I Uplift My Organisation's Cyber and Data Readiness? In: Ministry of Health Singapore. Available at: https://bit.ly/4eBP59T. Accessed 16 October 2024.

10. Guide on Managing and Notifying Data Breaches Under the Personal Data Protection Air. In: Personal Data Protection Commission Singapore. Available at: https://bit.ly/4h5nLT5. Accessed 16 October 2024.

11. Medical Information & Other Non-Clinical Information in Medical Records Subject to PDPA's Mandatory Data Breach Notification Requirements. In: Ministry of Health Singapore. Available at: https://bit.ly/498kBKE. Accessed 27 November 2024.