Baker McKenzie Wong & Leow

Healthcare & Life Sciences
Singapore

Data Privacy in Healthcare

Big data, cloud computing and cross-border transfers of personal data – these data privacy issues in healthcare have come to the fore in recent years, with a renewed focus on data privacy and the protection of personal data in the region.

These trends, combined with the vast amounts of patient personal data stored; the increasing number of medical devices connected to networks; and the fact that these medical devices are not usually designed with security as a priority have led to a notable prevalence of cyberattacks in the healthcare sector.

Personal Data In Singapore

In Singapore, "personal data" is defined very broadly, i.e. any data by which a person may be identified, whether the data is viewed in isolation or in conjunction with other data. The following legislation and guidelines apply to personal data in Singapore, to regulate the collection, use, disclosure and care of any such personal data:

- Personal Data Protection Act 2012 (PDPA);
- Personal Data Protection Regulations 2021;
- Personal Data Protection (Notification of Data Breaches) Regulations 2021; and
- Advisory Guidelines issued by the Personal Data Protection Commission, particularly the Advisory Guidelines for the Healthcare Sector.

Awards & Accolades

Band 1 for Life Sciences
Chambers Asia Pacific, Asia Pacific Region 2014 - 2025

Medical and Healthcare Law Firm of the Year
Asian Legal Business Southeast Asia Law Awards 2020 and 2021

Band 1 for Intellectual Property
Chambers Global, Asia Pacific Region 2009 - 2025

Band 1 for Intellectual Property
Chambers Asia Pacific, Singapore 2010 - 2025

Tier 1 for Intellectual Property
Legal 500 Asia Pacific, Singapore 2010 - 2025

Tier 1 for Patents and Copyrights/Trademarks in Singapore
ALB Asia IP Rankings 2018 - 2025

Asia Pacific Patents Firm of the Year
Asia IP Law 2023

Asia Pacific Trademark Firm of the Year
Asia IP Law 2024

Tier 1 for Trademark Contentious and Trademark Prosecution in Singapore
Asia IP Law 2025

Singapore: Copyright & Design; Trade Mark Prosecution Firm of the Year
Asia Pacific: IP Law Firm of the Year (Foreign Firms)
Managing IP Asia Pacific Awards 2024

IP Transactions & Advisory Firm of the Year
Managing IP Asia Pacific Awards 2021 and 2023

Copyright & Design Firm of the Year
Managing IP Asia Pacific Awards 2019 – 2023

Global IP Firm of the Year
Managing IP Asia Pacific Awards 2017, 2018 and 2022

The healthcare-specific Advisory Guidelines issued by the Personal Data Protection Commission (PDPC) further apply the key obligations under the PDPA and the Do Not Call provisions to scenarios that healthcare service providers may face. In particular, it contains guidance on the following:

- Scope of consent / deemed consent given by the patient;
- Retaining medical records of patients in light of the retention limitation obligation under the PDPA;
- Taking family histories when personal data of third-parties is required;
- Applicable exceptions to the consent, use and disclosure of personal data;
- Providing personal data when an individual requests access to his medical records, and how corrections to the personal data should be dealt with; and
- Obligations under the Do Not Call provisions when contacting patients or former patients.

The PDPA also contains specific exemptions to the obligation to obtain consent prior to the collection, use and disclosure of an individual's personal data. There are also instances where the data in question may cease to be considered as personal data, such as where the data has been anonymized or sufficiently de-identified. The organisation which deals with such anonymized data generally need not be subjected to the extensive data protection obligations under the PDPA, and may freely transfer such anonymized data out of Singapore.

Healthcare and Technology

To keep pace with rapid technological advancement and the growing popularity of telemedicine, which has led to medical devices becoming increasingly reliant on software for safe and effective function, the Health Sciences Authority (HSA) has also published its revised Regulatory Guidelines for Software Medical Devices and has finalised its Guidelines on Risk Classification of Standalone Medical Mobile Applications and Qualification of Clinical Decision Software. These guidelines offer guidance to address potential queries that medical device manufacturers and suppliers may have in relation to the risk classification, pre-market registration, and change notification requirements of their software medical device products.

The Cyber Security Agency of Singapore, Ministry of Health, HSA, and Integrated Health Information Systems have also developed the Cybersecurity Labelling Scheme for Medical Devices (CLS (MD)). The CLS (MD) applies to medical devices that handle health-related data or can connect to other devices, systems and services, and aims to allow consumers and healthcare providers to make informed purchases, and to incentivise manufacturers of such medical devices to adopt a security-by-design a pproach when developing their products.

Data Breach Incidents and Requirements

Given the global operations of large healthcare companies, it is natural that data privacy issues also tend to spread across multiple jurisdictions through cloud computing and cross-border data transfers. This is only intensified with the increasing number of connected medical devices and reliance on software. In turn, this interoperability increases companies' exposure and risk of being the subject of a cyberattack and data breach incident.

In addition to the obligations under the PDPA, there are strict data breach notification timelines. Generally, when there is a data breach incident, companies must first assess whether the data breach is a notifiable one. A data breach is notifiable if it results in (or is likely to result in) significant harm to the affected individuals, or it is (or is likely to be) of a significant scale. The affected company must conduct the assessment expeditiously and without unreasonable delay within 30 calendar days, and the PDPC must be notified no later than 3 calendar days after the company assesses the data breach to be notifiable.

The PDPC strongly enforces the data breach notification obligation, where it has released a self-assessment tool for companies and a guide on managing and notifying data breaches.

* * * * *

We are no stranger to navigating complexities across jurisdictions.

Baker McKenzie has a legal network spanning 45 countries. Within Asia Pacific, we have a large footprint, particularly in the healthcare industry, as we advise and act for the largest and leading global companies.

Our pharmaceuticals and healthcare industry group in the Asia Pacific region comprises more than 100 people with experience and specialist knowledge of the particular needs of the industry, enabling us to advise on the best ways to bring value to your business.

Contact Us

Andy Leck
Principal
Tel: +65 6434 2525
Fax: +65 6337 5100
andy.leck@bakermckenzie.com

Ren Jun Lim
Principal
Tel: +65 6434 2721
Fax: +65 6337 5100
ren.jun.lim@bakermckenzie.com

Ken Chia
Principal
Tel: +65 6434 2558
Fax: +65 9669 6421
ken.chia
@bakermckenzie.com

bakermckenzie.com

Baker McKenzie Wong & Leow
8 Marina Boulevard #05-01
Marina Bay Financial Centre, Tower 1
018981 Singapore
Tel: +65 6434 2606
Fax: +66 6338 1888