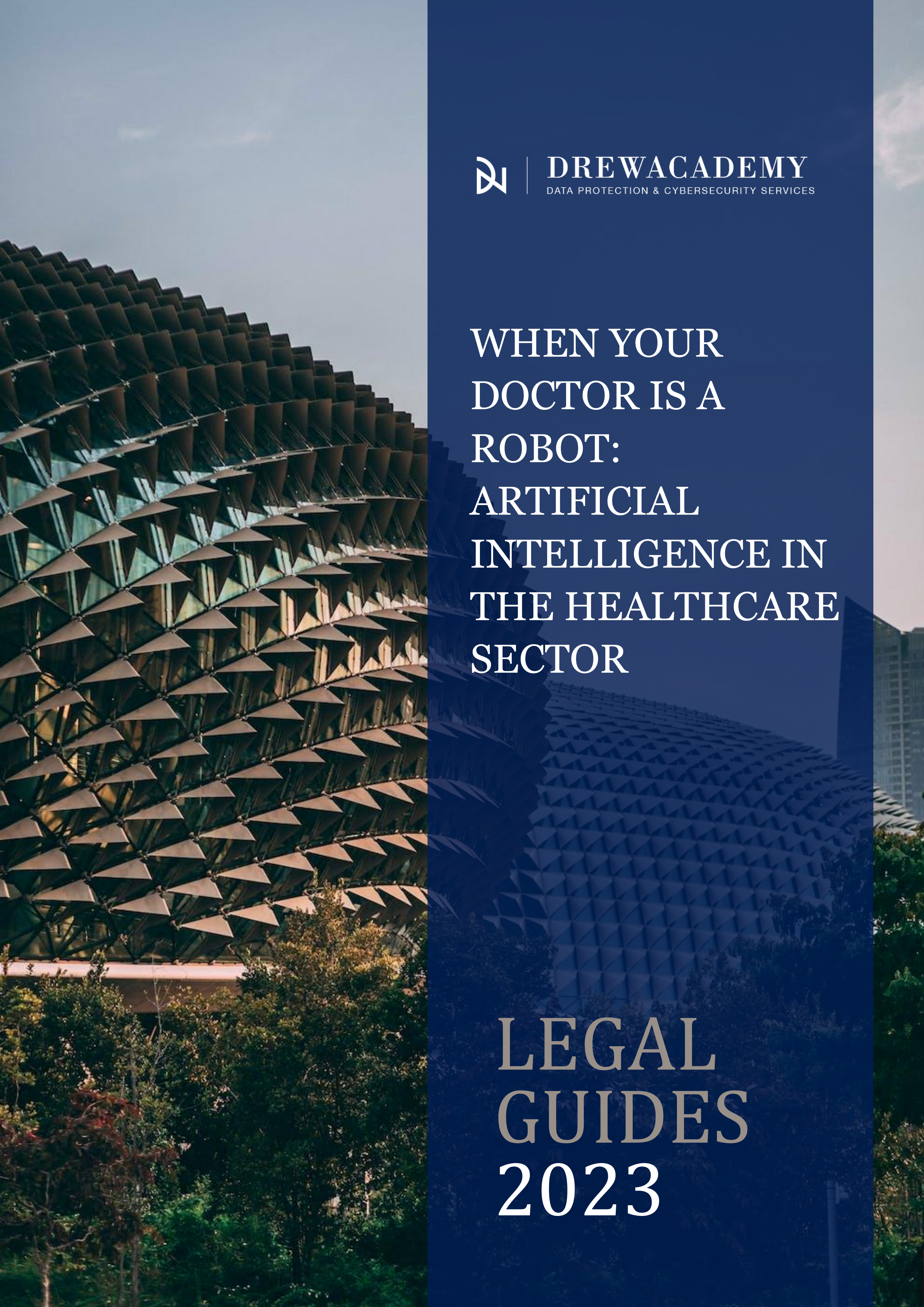

DREWACADEMY
DATA PROTECTION & CYBERSECURITY SERVICES

WHEN YOUR DOCTOR IS A ROBOT: ARTIFICIAL INTELLIGENCE IN THE HEALTHCARE SECTOR

LEGAL GUIDES
2023

CONTENTS

Developments as of 11 April 2023

WHEN YOUR DOCTOR IS A ROBOT: ARTIFICIAL INTELLIGENCE IN THE HEALTHCARE SECTOR

The development and use of artificial intelligence ("AI") technology has had an undeniably powerful and important impact on the healthcare sector. AI medical devices (which are artificial intelligence solutions intended to be used for medical purposes, regardless of whether the software is embedded in a medical device)[1] have been developed for medical diagnosis and predictive analysis purposes, which can drastically improve patient outcomes. Some examples of medical developments include AI that can highlight tumors on radiology scans of cancer patients,[2] detect eye diseases,[3] and even invent drug molecules fit for clinical trials.[4] It is hence unsurprising that the AI healthcare market has been projected to be worth US$102.7 billion by 2028.[5]

While there may be many exciting medical breakthroughs on the horizon, the use of AI in healthcare invariably comes with its fair share of novel legal issues. These issues need to be grappled with quickly, so that our laws keep pace with the technological advances.

Legal liability: who's to blame for AI errors?

As with the use of any technology, AI medical devices carry the risk of producing erroneous results or malfunction, which may harm the patient. In 1980, Therac-25, a computer-controlled medical device used to target and destroy cancerous tissue, delivered fatal doses of radiation to patients due to a glitch in computer coding. Several of the surviving victims and families of the deceased filed lawsuits in US courts against the designer and manufacturer of Therac-25, as well as the medical facilities using Therac-25. All these suits were eventually settled out of court.

Given the increasingly widespread development and use of AI medical devices, it is more than likely that errors will occur, and similar liability issues will have to be dealt with. However, AI medical devices capable of machine learning are inherently different from devices such as Therac-25, which are programmed to perform a limited set of tasks within a given set of instructions and rules. This means that some AI systems (i.e., those that may develop solutions by itself based on data that is fed to it) can potentially come to conclusions or suggest solutions inexplicable to humans. In such a situation, would there still be grounds to hold the AI designers, manufacturers, medical professionals, or medical facilities liable for errors made by the AI? More importantly, who should be held liable for paying damages to the victims?

Where there is no clear-cut direction to attribute liability, it may make practical sense to hold liable the entities that have the means of insuring themselves against such situations. For instance, under section 36(7) of the Medical Registration Act 1997, doctors may be required to take out mandatory insurance for indemnity against loss arising from medical negligence claims. However, in Singapore, there are no laws that may be interpreted as imposing strict liability on the use of AI medical devices. Turning to the common law, our established principles of vicarious liability and non-delegable duties may also be of limited applicability.

It has been held by the Singapore Court of Appeal that a defendant may be held vicariously liable for the tortious acts of its employee, committed in the course of employment to the extent that it is fair and just to impose liability on the defendant.[6] However, the AI device cannot be an 'employee', given that it is not a legal person and hence incapable of committing a tortious act. This results in an inconsistent outcome with a functionally equivalent situation where only a human doctor is involved, and the hospital

[1] Refer to the definition of "AI-medical device" in section 1.4 of HSA's Regulatory Guidelines for Software Medical Devices – A Life Cycle Approach, available at: https://www.hsa.gov.sg/docs/default-source/hprg-mdb/guidance-documents-for-medical-devices/regulatory-guidelines-for-software-medical-devices---a-life-cycle-approach_r2-(2022-apr)-pub.pdf, and the definition of "medical device" in the Health Products Act 2007.
[2] https://news.microsoft.com/en-gb/2020/12/09/a-microsoft-ai-tool-is-helping-to-speed-up-cancer-treatment-and-addenbrookes-will-be-the-first-hospital-in-the-world-to-use-it/
[3] https://healthitanalytics.com/news/google-backed-deepmind-creates-deep-learning-cds-for-eye-diseases
[4] https://investors.exscientia.ai/press-releases/press-release-details/2021/exscientia-announces-second-molecule-created-using-ai-from-sumitomo-dainippon-pharma-collaboration-to-enter-phase-1-clinical-trial/Default.aspx
[5] https://www.marketsandmarkets.com/Market-Reports/artificial-intelligence-healthcare-market-54679303.html
[6] *Skandinaviska Enskilda Banken AB (Publ), Singapore Branch v Asia Pacific Breweries (Singapore) Pte Ltd* [2011] 3 SLR 540

is liable for that human doctor's actions under the doctrine of vicarious liability.[7] In which case, the doctrine of non-delegable duties may be more relevant as it focuses instead on the relationship between the patient and the defendant, rather than the entity that committed the tort. It has been held by the Singapore Court that hospitals and doctors may owe non-delegable duties to a patient under their care, supervision or control, if it is fair, just, and reasonable to do so.[8] The court will consider factors such as whether the patient was a vulnerable person who placed himself under the hospital's direct care, supervision and control, and if the medical professional / medical facility had assumed a positive duty of care over the patient.[9]

What is the appropriate standard of care for medical diagnosis and treatment using AI tools?

In Singapore, the *Bolam-Bolitho* test is used to determine the legal standard of care in relation to medical diagnosis and treatment. The *Bolam*[10] test provides that a doctor is not negligent if they acted in accordance with a practice accepted by a responsible body of medical professionals. If the *Bolam* test is satisfied, the court will apply the *Bolitho*[11] test, which requires a consideration of whether this accepted practice passes a threshold test of logic, weighing the risks and benefits to reach a defensible conclusion.

However, there are inherent issues with applying the *Bolam-Bolitho* test for standard of care in relation to AI medical diagnosis and treatment. According to the *Bolam* test, a doctor is not negligent if he acted in accordance with a practice accepted by a responsible body of doctors. In the realm of novel AI tools and emerging technology, there may not be a substantial body of accepted practice to scrutinize in the first place.[12] Even if the *Bolam* test can be satisfied, difficulties also arise with applying the *Bolitho* test, which requires the court to consider if the medical opinion is logical and consistent. In the realm of AI decision-making, particularly with respect to unsupervised machine learning, the AI device's conclusions may prove inscrutable even to experts. The opacity of medical AI may make it difficult for experts to justify their opinions in considering the comparative benefits and potential risks from the use of medical AI.[13]

Informed consent in the context of AI diagnosis and treatment

The opacity of medical AI raises concerns in the context of informed consent as well. If the AI's decisions are inscrutable even to the medical professionals, how are medical professionals to convey the scope of diagnosis and treatment, to fully advise patients of the outcomes and risks, such that the patient understands the benefits and risks of the treatment before agreeing to it? In this regard, the Singapore Ministry of Health ("**MOH**") has published guidelines applicable to both developers and users of AI devices. Key to these guidelines is an overarching principle of transparency, which requires end users of the AI devices (medical practitioners and patients) to be given sufficient information to make informed decisions over the implementation of the AI device in the delivery of care[14]. In particular, MOH stipulates that AI developers should demonstrate the effectiveness of the AI tool and endeavor to ensure a sufficient level of explainability based on what the end user requires. For medical practitioners, this would mean clarity in recommendations, algorithmic decisions of the AI device, and concurrence that these are in-line with their current clinical practices. For patients, this would mean trust that the care rendered via the AI device is safe, and that they will not be "worse off" after the treatment.[15]

[7] https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/DV/2020/01-09/AI-report_EN.pdf at 35.
[8] *Hii Chii Kok v Ooi Peng Jin London Lucien* [2016] 2 SLR 544 at [77]
[9] *Woodland v Swimming Teachers Association and others* [2013] 3 WLR 1227
[10] *Bolam v Friern Hospital Management Committee* [1957] 1 WLR 582, 587.
[11] *Bolitho v City and Hackney Health Authority* [1998] AC 232.
[12] Chan, Gary Kok Yew. Medical AI, standard of care in negligence and tort law. (2021). AI, Data and Private Law: Translating Theory into Practice 173-198, at 179.
[13] Chan, Gary Kok Yew. Medical AI, standard of care in negligence and tort law. (2021). AI, Data and Private Law: Translating Theory into Practice 173-198, at 179.
[14] Sections 5.2.2 and 5.4, MOH Artificial Intelligence in Healthcare Guidelines.
[15] Section 4.7, MOH Artificial Intelligence in Healthcare Guidelines.

Safety standards for AI healthcare tools

In Singapore, the manufacture, import, supply, presentation and advertisement of health products (which include medical devices) in Singapore is robustly regulated under the Health Products Act 2007 ("**HPA**") and the Health Products (Medical Devices) Regulation 2010 (the "**Regulations**"). The use of AI medical devices requires the approval of the Health Sciences Authority ("**HSA**"), as these presumably fall under the category of 'medical devices' as stated in the HPA. Under the Regulations, the HSA may register a medical device if it is satisfied that the "*overall intended benefits to an end-user of the medical device outweigh the overall risks*" and it is "*suitable for its intended purpose and that any risk associated with its use is minimised*".[16] The HSA's Regulatory Guidelines for Software Medical Devices sets out additional information that must be submitted when registering an AI medical device, such as information on the datasets used to train the AI model, a description of the machine learning model used in the AI medical device, the test performance of the AI medical device, and how the AI medical device will be monitored and updated after it is deployed.

For continuous learning AI devices, complete information on the learning process including the process controls, verification, and ongoing model monitoring measures must be clearly presented for review in the application for registration of the AI device.[17] Once any AI medical devices are deployed in the real-world environment, active monitoring, review and tuning are crucial. Developers and distributors are required to establish a process in collaboration with the implementers and users to ensure traceability and also implement mechanisms to monitor and review the performance of the AI-MD deployed in clinical settings.[18]

Regulations over AI medical devices are steadily being developed elsewhere in the world as well. In the US, the Food and Drug Administration has recently released new guidance recommending that some artificial intelligence-powered clinical decision support tools, like sepsis prediction devices, should be regulated as medical devices.[19] The European Union plans to impose additional requirements on the use of AI in medical technology as such medical devices are considered "high risk AI systems", and issue fines for noncompliance. In this regard, the European Union plans to issue fines of up to €30 million ($36 million) or, if the offender is a company, up to 6% of its total worldwide annual turnover for infringing the rules.[20]

Data protection and cybersecurity concerns for AI healthcare devices

An increasing number of healthcare devices such as smart watches, medical sensors, and fitness trackers are connected to the Internet[21], which is useful for inpatient and outpatient monitoring - they can help medical professional streamline workflows and improve quality of life for patients. However, this connectivity also makes them vulnerable to attacks from bad actors. There have been instances of attackers spamming repeat messages to cardiac devices in order to deplete the battery. An even more extreme example of cybersecurity compromise was demonstrated by researchers showing how attackers could potentially access a Medtronic pacemaker remotely, and administer or withhold shocks to patients.[22]

As AI medical devices collect and use vast amounts of data to analyse, there will inevitably be similar concerns over the data protection and cybersecurity measures that have been implemented in and around these devices.

[16] Regulation 25, Health Products (Medical Devices Regulations) 2010
[17] Section 9.2, HSA Regulatory Guidelines for Software Medical Devices (https://www.hsa.gov.sg/docs/default-source/hprg-mdb/guidance-documents-for-medical-devices/regulatory-guidelines-for-software-medical-devices---a-life-cycle-approach_r2-(2022-apr)-pub.pdf)
[18] Section 9.3, HSA Regulatory Guidelines for Software Medical Devices
[19] https://healthitanalytics.com/news/fda-releases-guidance-on-ai-driven-clinical-decision-support-tools
[20] https://ec.europa.eu/newsroom/dae/items/709090
[21] These network-enabled devices are collectively referred to as the "Internet of Things" or "IoT".
[22] https://www.techtarget.com/iotagenda/feature/Healthcare-IoT-security-issues-Risks-and-what-to-do-about-them

In Singapore, the Ministry of Health's guidelines on the use of AI states that developers should ensure that the AI medical device can prevent, detect, respond and where possible recover from foreseeable cybersecurity risks. In particular, developers should adopt a "Security by Design" approach when developing the AI product.[23] The Singapore Personal Data Protection Commission's Advisory Guidelines for the Healthcare Sector also recommend the de-identifying of data. In situations where certain individual characteristics need to be retained, developers can consider anonymisation techniques to protect this data (e.g., data masking, pseudonymisation, data perturbation).[24]

Conclusion

The use of AI in the healthcare sector promises more personalized treatment, faster diagnosis, and a higher likelihood of finding a cure for or diagnosis of a condition, because AI is able to process data and derive insights at a speed and depth beyond what a human is able to do. However, issues surrounding its use have not been fully ironed out yet, such as legal liability, the extent of informed consent, and data protection and cybersecurity issues. It is thus important for organisations to continue monitoring developments in this space to ensure that their use of AI minimizes the risk to human safety as much as possible, so that humans are not worse off for having used AI in their medical diagnosis and treatment.

Drew Academy wishes to acknowledge our Senior Associate Lim Shao Min for assisting in the preparation of this article.

The content of this article does not constitute legal advice and should not be relied on as such. Specific advice should be sought about your specific circumstances.

[23] Section 4.6, Ministry of Health's Artificial Intelligence in Healthcare Guidelines (https://www.moh.gov.sg/docs/librariesprovider5/eguides/1-0-artificial-in-healthcare-guidelines-(aihgle)_publishedoct21.pdf)
[24] https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Sector-Specific-Advisory/advisoryguidelinesforthehealthcaresector28mar2017.pdf. See also section 4.6.3, Ministry of Health's Artificial Intelligence in Healthcare Guidelines.

DREW DATA PROTECTION & CYBERSECURITY ACADEMY

Drew Data Protection & Cybersecurity Academy (Drew Academy) was established in 2020 by Drew & Napier to help our clients build their capabilities and develop and implement organisational strategies, structures, policies and processes to meet their legal, regulatory and compliance obligations. Drew Academy offers a range of courses in areas such as data protection, cybersecurity, data governance and in-house commercial practice. A particular focus for us is the delivery of workplace learning solutions and development of customised training courses. We also offer outsourced DPO services and data protection consulting services through our experienced team of practitioners.

Drew Academy is helmed by Lim Chong Kin and David N. Alfred. Our course leaders are experienced in various aspects of data and cyber governance, data protection, cybersecurity engineering and in-house commercial practice.

ARTIFICIAL INTELLIGENCE AND DIGITAL TRUST

Drew & Napier’s Artificial Intelligence (AI) and Digital Trust practice brings together its expertise across several technology-related domains and in fields as diverse as data protection, cybersecurity, healthcare, Fintech, intellectual property and competition law (to name a few) to advise clients on the full range of legal issues relating to AI and Digital Trust. In addition to advising on commercial, regulatory and international / cross-border issues, our advice extends into areas such as governance and ethics as we seek to enable our clients to navigate areas where laws and legal principles are still emerging.

Working together with the Drew Academy, we provide solutions that reflect our deep understanding of underlying technologies, the risks and uncertainties involved and practical business considerations. Internationally, there is a growing consensus on AI governance.

For more information on our experience, please contact:

Lim Chong Kin
Managing Director, Corporate & Finance;
Co-Head, Data Protection,
Privacy & Cybersecurity Practice;
Co-Head, Drew Data Protection &
Cybersecurity Academy

T: +65 6531 4110
E: chongkin.lim@drewnapier.com

Benjamin Gaw
Director, Corporate and
Merger & Acquisitions;
Head, Healthcare & Life Sciences
(Corporate & Regulatory)

T: +65 6531 2393
E: benjamin.gaw@drewnapier.com

Cheryl Seah
Director, Corporate & Finance

T: +65 6531 4167
E: cheryl.seah@drewnapier.com

DREWACADEMY
DATA PROTECTION & CYBERSECURITY SERVICES

10 Collyer Quay
10th Floor Ocean Financial Centre
Singapore 049315

www.drewnapier.com/Academy

T: +65 6531 4152
F: +65 6535 4864
E: academy@drewnapier.com

In association with

DREW & NAPIER