Bird & Bird ATMD Life Sciences & Healthcare Update

Regulating Telehealth in Singapore – the New Frontier in Healthcare

The new frontier in healthcare is telehealth: the use of infocomm technology in providing healthcare services over physically separate environments.[1] This article examines the existing framework that regulates telehealth in Singapore and highlights emerging legal issues that merit further consideration. Proactive regulatory measures kept apace with the advances in telehealth will help to maximise telehealth's potential while balancing and safeguarding patients' interests.

Summary

From Uber to Oculus; Spotify to Siri; Airbnb to Alexa – transformative innovation (disruptive or otherwise) pervades our daily lives. *Telehealth* is the latest buzzword in transformative innovation that is shaping the provision of healthcare. The benefits of telehealth are manifold. For example, telehealth can enable a doctor to remotely operate on a patient, or a patient to consult his doctor from the comfort of his home.[2]

The term "telehealth" and "telemedicine" are used interchangeably in some quarters. However, there is a distinction in the industry. "Telemedicine" refers to remote clinical services, whereas "telehealth" refers to the broader scope of health services including non-clinical services, such as health education.

There is no overarching legislation governing telehealth in Singapore; the regulatory regime comprises an accretion of various codes and guidelines, namely:

a National Telemedicine Guidelines ("**NTG**");

b Ethical Code and Ethical Guidelines ("**ECEG**") and Handbook on Medical Ethics ("**Handbook**"); and

c Telehealth Product Guidelines ("**TP Guidelines**").

The NTG, ECEG and Handbook are primarily concerned with patient safety in the telemedicine environment, while the TP Guidelines clarify when a telehealth product would be considered as a "medical device" subject to the Health Sciences Authority's control. Recently, the Ministry of Health proposed a new Healthcare Services Bill that will further regulate telemedicine.

Despite the regulations, there are broader legal issues that have yet to be addressed and merit further consideration, such as the following:

a What should be the licensure regime for overseas doctors providing telemedicine in Singapore?

b How should jurisdictional issues be determined in a case of tele-medical negligence?

c What cybersecurity measures should be in place for telehealth products?

As Singapore moves into telehealth as part of the Smart Nation initiative[3], regulators must keep apace with advances in digital health. Proactive regulations and timely implementations can unlock the full potential of the transformative technology.

1 Definition of "telehealth" is taken from the Health Sciences Authority's Telehealth Products Guidelines (August 2017) p 7.

2 In April this year, six hospitals in Singapore announced that they will provide consultation via video-conferencing for eligible patients to see their doctors from home. Another example is Doctor Anywhere, which is an app that allows users in Singapore to have virtual consultations with doctors.

3 More information on Singapore's telehealth initiative can be found here: < https://www.smartnation.sg/initiatives/Health/telehealth-integrated-and-seamless-healthcare-services-at-home>.

Existing Legal Framework for Telehealth

Guidelines	Highlights	Commentary
National Telemedicine Guidelines ("**NTG**")[4]	The NTG, issued by the Ministry of Health in 2015, sets out best practices in the following areas involved in the delivery of telemedicine: • clinical standards and outcomes; • human resources; • organisational; and • technology and equipment. The following are some notable guidelines: • Healthcare professionals intending to provide telemedicine services from or within Singapore must be registered and licensed with the respective regulatory and licensing body. • "Duty of care" must be established in all telemedicine encounters; Healthcare professionals should collaborate with each other to clarify their roles and responsibilities. • Telemedicine services must be provided as part of a structured system and the overall standard of care must not be less than what is given in conventional services. • Healthcare providers should obtain informed consent from the patient before starting any telemedicine services.	As the NTG is intended to only be a guide to the industry, it has no force of law. It remains to be seen whether the Ministry of Health would sanction a healthcare provider or organisation that does not comply with the NTG.
Ethical Code and Ethical Guidelines ("**ECEG**")[5] and Handbook on Medical Ethics ("**Handbook**")[6]	In late 2016, the Singapore Medical Council published revised ECEG and Handbook, effective 1 January 2017, to address emerging medical issues including telemedicine. The following are some examples of the requirements relating to telemedicine: • Doctors offering telemedicine must endeavour to provide the same quality and standard of care as in-person medical care. Otherwise, they must state the limitations of their opinions. • Doctors performing remotely guided medical procedures must have the necessary expertise to provide the remote guidance. • Doctors must take reasonable care to ensure confidentiality of medical information shared through technology and ensure compliance with the relevant laws on personal data. • Prior to obtaining consent, doctors must provide their patients with sufficient information about telemedicine. • Where patients need to operate telemedicine equipment, doctors must ensure the patients are sufficiently trained to do so.	Doctors in Singapore are to comply with the ECEG. Failure to meet the standards required under the ECEG may lead to disciplinary proceedings by the Singapore Medical Council. The Handbook supplements the ECEG, providing the rationale behind the ethical standards in the ECEG and explaining how doctors can achieve such standards.

4 The Ministry of Health, National Telemedicine Guidelines (January 2015).

5 The Singapore Medical Council, Ethical Code and Ethical Guidelines (2016 Edition)

6 The Singapore Medical Council, Handbook on Medical Ethics (2016 Edition).

Guidelines	Highlights	Commentary
Telehealth Product Guidelines ("**TP Guidelines**")[7]	In August 2017, the Health Sciences Authority ("**HSA**") issued the TP Guidelines regarding when a telehealth product would be classified as a medical device. The classification of a telehealth product as a medical device carries significant implications, because medical devices are stringently regulated by the HSA. The classification of a telehealth product hinges on the intended use of the device by the product owner. **Intended for medical purposes** Telehealth products intended for medical purposes must be registered as a medical device with the HSA. The following are medical purposes: *"purpose of investigation, detection, diagnosis, monitoring, treatment or management of any medical condition, disease, anatomy or physiological process".* **Not intended for medical purposes** Telehealth products that are not intended for medical purposes need not be registered as a medical device. For example, devices for general well-being (e.g. wearable pedometer) are not considered as a medical device. However, where a telehealth product is not intended for medical purposes, but can nevertheless perform the function, the onus is on the product owner to include a clarification statement that the product is not intended for medical purposes.	In practice, the classification of the telehealth product may not be clear-cut. For example, how will the HSA categorise a device intended for both "medical" and "general well-being" purposes? It may well be classified as a medical device by its medical purpose notwithstanding its other collateral purposes. Further, would the clarification statement protect the product owner if the HSA determines the telehealth product is in fact intended for medical purposes? Telehealth product developers may wish to take advantage of the recent Pre-Market Consultation Scheme[8] to consult the HSA on the classification of their telehealth product.

Emerging Legal Issues

Looking ahead, regulators should consider the broader legal ramifications arising from telehealth. The following are three legal issues that merit further consideration.

Licensure Regime for Overseas Doctors

The NTG indicates that doctors delivering telemedicine from or within Singapore are to meet the licensing requirements imposed by the country where the patient is residing. In the hypothetical scenario, if the UK doctor is required to comply with the existing local licensure regime to provide virtual medical consultations in Singapore, this could impede the adoption of telemedicine.

For telemedicine to achieve its full potential in Singapore, licensure requirements must be made simpler for overseas doctors while striving to balance the interests of the patient. Singapore may take guidance from how other countries, such as the US, have attempted to

Hypothetical Scenario

Three months ago, a doctor in the UK treated a patient in Hong Kong via a remote surgical system. Recently, the patient re-located to Singapore for work. In Singapore, the patient received virtual follow-up medical consultations with his UK doctor and began experiencing medical complications.

7 The Health Sciences Authority, Telehealth Products Guidelines (August 2017).

8 More information on the Pre-Market Consultation Scheme can be found here: http://www.hsa.gov.sg/content/dam/HSA/HPRG/Medical_Devices/Updates_and_Safety_reporting/Regulatory_Updates/Medical%20Device%20Pre-Market%20Consultation%20and%20Priority%20Review%20Scheme.pdf.

ease licensure requirements for telemedicine. In the U.S., each state has different licensure requirements, which has been a barrier for doctors to practice telemedicine across state lines. The Interstate Medical Licensure Compact ("**Compact**") was formed to create an expedited pathway to license qualified doctors to practice in multiple states. The objective of the Compact is to relieve the nation's growing shortage of doctors and to provide patients with better access to specialist care.

The Compact is not part of any federal government program, but is an agreement among states. As of 1 December 2017, at least twenty states have participated in the Compact or introduced the Compact.[9] Under the Compact, a doctor seeking to obtain a licence must meet certain requirements. For example, she must hold a full and unrestricted medical licence by a member state and have no history of disciplinary actions against her medical practice or any criminal record. Riding on the success of the Compact, the Physical Therapy Licensure Compact was recently formed in the U.S.

To date, there is no international licensing compact for doctors. Singapore could consider entering into partnership agreements with different countries to provide for an expedited pathway to license overseas doctors to practice telemedicine in Singapore and vice versa. Further, like the TP Guidelines which clarifies what telehealth products require registration as a "medical device", it is suggested that regulators could provide clarity on the activities undertaken by an overseas doctor which require licensing, and those which are exempt. For example, local licensing would not be required where the overseas doctor only provides virtual educational programs to patients or healthcare providers or gives suggestions, as an expert in the field, to a licensed doctor in Singapore.

Jurisdictional Issues in Telemedical Negligence

In the hypothetical scenario, would the Singapore court have jurisdiction over a telemedical negligence claim by the patient against his UK doctor? This would depend on whether Singapore is considered to be the natural forum. In Singapore, the courts have adopted the test set out in *Spiliada Maritime Corporation v Cansulex Ltd*[10] to determine the natural forum.[11] The test consists of two stages of inquiries: (i) which forum has the closest and most real connection with the dispute; and (ii) if there would be a denial of justice if the case is tried in that jurisdiction.

For tort claims, the place where a tort was committed is *prima facie* the natural forum.[12] In telemedicine, where the provision of medical services may be spread across multiple jurisdictions, the challenge will be to determine the place of the tort. In complex situations involving multiple jurisdictions, the courts have applied the "substance of tort" test, whereby they look back on the series of events and determine where in substance the cause of action arose.[13]

In the hypothetical scenario, the place of the tort can be difficult to pin-point. Is it in the UK where the doctor conducted the remote surgery? Or is it in Hong Kong where the patient received the surgery? Or is it in Singapore, where the patient had follow-up virtual consultations and began to experience medical complications? To complicate the matter, what if the patient's injury is *equally* caused by the doctor's negligence during the remote surgery and the follow-up consultations? How would the court determine where in substance the cause of action arose? Would the Singapore court ever consider dissecting the claim so that it would only hear the issue regarding the follow-up consultations which occurred when the patient was in Singapore and defer the issue regarding the remote surgery which occurred when the patient was in Hong Kong to another court?

There has yet to be a case regarding telemedical negligence in Singapore. It remains to be seen how the courts will determine the place of the tort, especially in complex multi-jurisdiction scenarios. However, as telemedicine advances and patients in Singapore receive treatment from doctors located in other countries, challenges regarding jurisdiction will inevitably arise. To create certainty, doctors may wish to enter into legally binding agreements with their patients regarding jurisdiction. Further, law-makers may consider legislating "long-arm" provisions that would subject every doctor outside of Singapore who practices telemedicine here to Singapore's jurisdiction. For example, in Malaysia the Telemedicine Act[14] imposes liabilities on doctors who breach the Telemedicine Act, notwithstanding that they are located outside of Malaysia.[15] To reinforce Singapore's jurisdiction, regulators can also consider as part of the licensure regime for overseas doctors to require all applicants to consent to the jurisdiction of Singapore.

---

9 The Interstate Medical Licensure Compact website <http://www.imlcc.org/> (accessed 13 October 2017)

10 [1987] AC 460.

11 Rickshaw Investments Ltd v Nicolai Baron von Uexkull [2007] 1 SLR 377.

12 Ibid.

13 Jio Minerals FZC v Mineral Enterprises Ltd [2011] 1 SLR 391.

14 Telemedicine Act 1997 (Act 564). The Telemedicine Act has yet been enacted in Malaysia.

15 Ibid. See section 3: "Any person who practises telemedicine in contravention of this section, notwithstanding that he so practises from outside Malaysia, shall be guilty of an offence and shall on conviction be liable to a fine not exceeding five hundred thousand ringgit or to imprisonment for a term not exceeding five years or to both."

Cybersecurity in Telehealth Products

Telehealth products, like all interconnected technology, are vulnerable to cyberattacks. Cybersecurity issues to telehealth products considered as "medical devices" can especially impact patient safety. The risk is real. In August 2017, Abbott Laboratories voluntarily recalled some 465,000 radio frequency-enabled pacemakers in the U.S. due to cybersecurity vulnerabilities, which could have allowed hackers to change the devices' pacing commands or prematurely deplete the batteries.[16]

The issue of telehealth products and cybersecurity is an emerging issue that has not been addressed in the TP Guidelines by the HSA. In the US, the FDA has taken some steps to set out guidance on cybersecurity measures for medical devices. In 2016, FDA issued a guidance document entitled "Postmarket Management of Cybersecurity in Medical Devices" ("**2016 Guidance**").[17] The 2016 Guidance targets medical devices that use software, including programmable logic and medical mobile apps that are considered as medical devices. The 2016 Guidance recommends manufacturers to monitor, identify and address cybersecurity vulnerabilities as part of their post-market management of the device. Specifically, manufacturers should develop cybersecurity risk management programs throughout the lifecycle of the medical device. The 2016 Guidance builds on the guidance document entitled "Content of Premarket Submission for Management of Cybersecurity in Medical Devices" issued in 2014.[18]

Recently, US Senator Richard Blumenthal (Connecticut) introduced a new cybersecurity legislation focused on medical devices.[19] The aim of the legislation is to ensure patient safety during cyberattacks on medical devices. Under the bill, manufacturers of medical devices would be required to create a cyber report card, mandate product testing before sale, increase remote access protection, provide fixes and updates for free, and follow certain procedures for end-of-life medical device.

Singapore has taken steps to counter cybersecurity threats. The Ministry of Communications and Information and the Cyber Security Agency of Singapore recently proposed a Cybersecurity Bill.[20] The bill applies across all sectors. It provides a framework for the regulation of "critical information infrastructures" for the continuous delivery of "essential services", which includes healthcare. The powers of the bill will be vested in a Commissioner of Cybersecurity who will determine which computer system is a "critical information infrastructure". As the bill stands, it is unlikely to have a direct impact on telehealth products which most likely will not be considered as part of a "critical information infrastructure".

Therefore, it is recommended that regulators provide guidance to the industry on what cybersecurity measures should be introduced before a telehealth product is placed in the hands of a user, as well as what actions need to be taken in the event of a cybersecurity attack. It may well be that the cybersecurity measures differ depending on whether the telehealth product is considered as a medical device or a device for general well-being. Further, to increase consumer's confidence in telehealth products, regulators should consider creating an independent watchdog with expertise in telehealth to track the safety of the device, particularly regarding cybersecurity vulnerabilities.

Concluding Remarks

As with any new transformative technology, there will be a constant tension between proponents of a laissez faire approach and those in favour of a stringent regulatory regime. Telehealth is no exception. Thus far, Singapore has adopted a light-touch approach and introduced regulations incrementally to address specific aspects of telehealth. However, unregulated aspects of telehealth could negatively impact the value of telehealth. Proactive regulatory measures kept apace with the advances in digital health will help to maximise telehealth's potential, balance and safeguard patients' interests, and boost user confidence in telehealth products and services.

This article was first published in the Singapore Law Gazette December 2018 issue.

16 Michael Erman, "Abbot releases new round of cyber updates for St. Jude pacemakers", Reuters (30 August 2017) < https://www.reuters.com/article/us-abbott-cyber/abbott-releases-new-round-of-cyber-updates-for-st-jude-pacemakers-idUSKCN1B921V> (accessed 9 October 2017).

17 The U.S. Food & Drug Administration, Postmarket Management of Cybersecurity in Medical Devices, Guidance for Industry and Food and Drug Administration Staff (28 December 2016).

18 The U.S. Food & Drug Administration, Content of Premarket Submission for Management of Cybersecurity in Medical Devices, Guidance for Industry and Food and Drug Administration Staff (2 October 2014).

19 The bill can be assessed here: https://www.congress.gov/115/bills/s1656/BILLS-115s1656is.pdf.

20 The bill can be assessed here: https://www.csa.gov.sg/~/media/csa/cybersecurity_bill/draft_cybersecurity_bill_2017.ashx?la=en.

Get in touch

If you have any queries, please do not hesitate to contact any of our following lawyers from the Life Sciences & Healthcare Sector Group:

Alban Kang
Partner
Bird & Bird ATMD

Tel: +65 6428 9828
alban.kang@twobirds.com

Tai Yuet Ping
Partner
Bird & Bird ATMD

Tel: +65 6428 9820
yuetping.tai@twobirds.com

twobirds.com

Aarhus & Abu Dhabi & Amsterdam & Beijing & Bratislava & Brussels & Budapest & Copenhagen & Dubai & Dusseldorf & Frankfurt & The Hague & Hamburg & Helsinki & Hong Kong & London & Luxembourg & Lyon & Madrid & Milan & Munich & Paris & Prague & Rome & Shanghai & Singapore & Stockholm & Sydney & Warsaw