Medicine and the Law

TELEMEDICINE (PART 2)

Text by Jansen Aw and Dr Alex Cheng Wei Ray

This is the second article of a two-part series. In this, the authors delve deeper into the legal-technological aspects surrounding the use of telemedicine. Part 1 (https://bit.ly/5305-Insight) discusses issues where law and technology converge in the realm of telemedicine.

Due diligence and authentication issues

It is not often that a doctor is faced with considerations of due diligence to be carried out with regard to a patient. These belong more commonly to a corporate setting. Nevertheless, there is a need to carry out due diligence and authentication of a patient in the context of telemedicine. Given the remote environment in which the doctor comes into contact with the telemedicine user, it may be difficult for a doctor to verify the identity of the patient and the information provided, and this may lead to a risk of abuse. For example, a user may provide false information to a doctor over the telemedicine platform in order to obtain a payout under an insurance policy, and it may be difficult for the doctor to verify such information given that they are not in direct contact with the patient.

The current National Telemedicine Guidelines (NTG) stipulates that a doctor should request for the patient's photo identification with NRIC/FIN number clearly shown on the video screen before the consultation to verify their identity. However, a colour photocopy of an edited identity card will look exactly the same as a real one on screen, as the doctor will not be able to feel the texture of the card. Furthermore, since the various telemedicine apps operate on their own servers, there are also no alternative avenues for a doctor to check if an NRIC/FIN is genuine.

One solution would be to implement a two-factor authentication system, where not only the patient's identification document is verified, but the patient's identity can be verified using their mobile number. Additionally, as a government-wide initiative, it may make sense if Singpass can be integrated into telemedicine apps during the initial registration to automatically verify a patient's identity, similar to how some banks are getting information from the MyInfo platform to verify new account signups.[1] Alternatively, an NRIC/FIN verification platform can be created to grant doctors the right to check if the identification number is genuine. This will in turn prevent issues regarding phantom patients and any potential drug abuse cases.

IT security and confidentiality issues

At the moment, tele-consultations are performed across various platforms. Some GPs and even polyclinics are conducting them through the use of video-conferencing software, which may pose a security concern. It would be wise for a telemedicine provider to have in place the proper infrastructure and IT security to ensure that information transmitted between the doctor and patient is secure from intruders or hackers.

In line with the above, telemedicine providers should also ensure that there are proper Identity and Access Management[2] mechanisms in place to prevent unauthorised access to the telemedicine application and patient records and to prevent any identity impersonation where possible.

Additionally, there are confidentiality issues surrounding telemedicine. Although the NTG guidelines state that doctors should not record the contents of the tele-consultation to respect the sanctity of doctor-patient confidentiality, there is nothing stopping the patients from doing the same thing on the other end, which may make some doctors uncomfortable in providing care via tele-consultation. A proposed solution in future, once the Healthcare Services Act kicks in, is that tele-consultation should only be conducted on approved applications with all these considerations taken into account.

Data protection

If telemedicine is the engine driving the way forward in providing medical services, then data (or more specifically, the patient's data) is the fuel that powers this engine. It is through the collection and use of such patient data over remote means that the doctor is able to come up with the relevant diagnosis, treatment and advice for the patient in telemedicine.

In this regard, it is critical that a doctor providing telemedicine services be well versed in the requirements to protect personal data of the patient under the Personal Data Protection Act (PDPA). These include ensuring

that the patient's consent is obtained before collecting, using or disclosing his/her data; ensuring that there are reasonable security arrangements to protect such personal data; ensuring that the personal data of the patient is accurate during collection; and ensuring that the personal data of the patient is not retained for an unreasonably long time.[3] It should be noted that the PDPA will be undergoing changes in the future, and a public consultation has recently been carried out to seek comments on these proposed changes.[4]

The future of telemedicine

In a recent McKinsey survey, healthcare leaders interviewed cited remote monitoring as a key area for future investment and up to $250 billion worth of current US healthcare spending could potentially be virtualised.[5] If devices can be created to replicate a doctor's physical examination and provide accurate information to the attending physician remotely, even telemedicine's staunchest opponents may be converted to embrace it. Some of these technologies already exist but cost issues prohibit their widespread adoption in telemedicine. It may just be a matter of time before such production costs are lowered, making telemedicine more accessible to patients. For example, oDocs Eye Care invented an add-on device that can turn any smartphone camera into an ophthalmoscope, which can aid doctors in diagnosing eye conditions through tele-consultation.[6] Electronic stethoscopes which can wirelessly transmit recordings of auscultation sounds back to the computer via Bluetooth are also available in the market. Perhaps in future, every telemedicine patient can have an electronic stethoscope at home to complement the tele-consultation.

Artificial intelligence (AI) is also becoming more pervasive in telemedicine. There are currently several online self-diagnosis programs available (eg, Symptom Checker by WebMD and the Mayo Clinic Symptom Checker), which taps into AI technology that allows patients to self-diagnose their medical condition. In our view, the market for smart tele-monitoring devices with incorporated AI technology is set to grow.

However, these come with challenges too. Deepfakes, which refer to manipulated videos or other digital representations produced by sophisticated AI that yield fabricated images and sounds that appear to be real, may also pose a problem in the arena of telemedicine.[7] Doctors may have problems verifying a patient's identity, giving rise to phantom patients. It may even be exploited as a loophole by patients with ill intent to manipulate the tele-consultation process.

Recently, Singapore's Infocomm Media Development Authority and Personal Data Protection Commission (PDPC) produced the second edition of the Model AI Governance Framework (Model Framework) to regulate the use of AI technology.[8] The Model Framework's strength and unique contribution to the global discourse on AI ethics lies in translating ethical principles into practical recommendations that organisations can readily adopt to deploy AI responsibly. The barrier to entry of AI adoption is hence lowered and users have the confidence to implement AI to improve their processes. This framework is *sui generis*, which means that the framework can even be applied in the field of medicine. Therefore, using the PDPC's Model Framework as the foundation, we hope that the Ministry of Health comes up with guidelines specifically for telemedicine, accompanied by a compendium of use-cases, to guide practitioners in their practice of telemedicine.

Conclusion

Telemedicine has the potential to reshape the way in which medical practitioners practise medicine. Just like how Uber disrupted the transport sector, how AirBnB disrupted the tourism industry and how blockchain technology disrupted the banking sector, it would be interesting to see whether telemedicine will become the next disruptor in the practice of medicine in the age of the COVID-19 pandemic. ◆

Jansen is a partner with the Litigation and Dispute Resolution Practice, and Technology and Data Protection Practice in one of the oldest law firms in Singapore, Donaldson & Burkinshaw LLP. Jansen is an advocate and solicitor of the Supreme Court of Singapore.

Dr Alex is a family physician who works as a locum medical doctor during his free time. He is currently pursuing a Master of Laws with the University of London. Aside from his medical qualifications, he also holds the degrees of Bachelor of Laws, Master of Professional Accounting and Master of Business Administration. He is an incoming practice trainee lawyer at Donaldson & Burkinshaw LLP.

References

1. GovTech Singapore. MyInfo. Available at: https://bit.ly/35EnOhv.

2. Gittlen S, Rosencrance L. What is identity and access management? Guide to IAM. TechTarget SearchSecurity [Internet]. Available at: https://bit.ly/3mrITqz.

3. Personal Data Protection Act 2012. Available at: https://bit.ly/31SrX39.

4. Personal Data Protection Commission. Public Consultation on Personal Data Protection (Amendment) Bill. Available at: https://bit.ly/3fTgJUf.

5. Bestsennyy O, Gilbert G, Harris A, Rost J. Telehealth: a quarter-trillion-dollar post-COVID-19 reality? McKinsey & Company [Internet]. 29 May 2020. Available at: https://mck.co/3cW5mZR.

6. oDocs Eye Care. About us. Available at: https://bit.ly/3usH0N7.

7. Shao G. What 'deepfakes' are and how they may be dangerous. CNBC [Internet]. 13 October 2019. Available at: https://cnb.cx/3wJWjDk.

8. Personal Data Protection Commission. Singapore's Approach to AI Governance. Available at: https://bit.ly/3fJiYcO.