

# TIME IS BRAIN:

## Stoking Cybersecurity in Strokes

Text by Dr Chia Ghim Song

Every medical student has been taught that the four basic principles of medical ethics are non-maleficence, beneficence, patient autonomy and social justice. Indeed, these four principles are enshrined in the Singapore Medical Council Ethical Code and Ethical Guidelines itself. These four principles are also commonly described as the Beauchamp and Childress' Principles of Biomedical Ethics, named after the two ethicists who first came up with these principles.

The difficulty of applying these four principles in real-life medical practice is that no one principle holds absolute sway over the other three in most circumstances. There are almost always trade-offs between all four principles, with one or two principles being pre-eminent. Which principles hold pre-eminence would depend on how the facts turn in each situation.

A good example of this is the use of telemedicine and IT in acute stroke management. As a neurointerventional radiologist, one of the most clinically rewarding, but at the same time stressful and demanding, area of our work would be in the realm of acute ischemic stroke interventions.

Together with an excellent multi-disciplinary team of stroke neurologists, emergency physicians, anaesthesiologists, nurses, radiographers and paramedics,

we strive to assess, image, identify and transfer stroke patients with a large vessel occlusion (LVO) to the angi-suite for endovascular thrombectomy (EVT) to remove the clot as quickly as possible.

AI-enabled stroke solutions that automatically detect the presence of an LVO and alert all members of the stroke team within minutes of a stroke patient being scanned have been adopted by many leading institutions in the world. As most stroke patients present after hours, these elegant solutions (which reside in a phone app) automatically notify and allow all parties to simultaneously access the anonymised images at the touch of a button while off-site. Rapid decisions can be made and care of the patient can be immediately coordinated, resulting in significantly shortened time to treatment. However, implementation of these stroke AI mobility solutions is fraught with challenges in our current cybersecurity landscape and with internet separation.

### Time is brain

Life as a neurointerventional radiologist used to be more peaceful. This was until 2015, when a series of randomised controlled trials demonstrated significant benefit of performing EVT in selected patients presenting with LVO acute ischemic stroke. The treatment was highly efficacious with a number needed to

treat of three; ie, one in three stroke patients benefited from such treatment. As they say, the rest (of our social life after circa 2015) was history.

But for EVT to be as efficacious as it could be, time is of the essence. The faster we take the clot out, the shorter the ischemic time, and the better our patient's outcome. "Time is brain" became our new mantra. Cost-benefit studies have shown that every minute saved correlates to approximately 1,000 USD of net monetary benefit to the patient and the healthcare system.<sup>1</sup> Hence, significant effort was invested into streamlining the workflow/decision-making process and enhancing the coordination between specialists to minimise the delay to treatment.

### AI-enabled solutions

Industry has been quick to ride the AI revolution and create software solutions that automatically analyses the anonymised CT/CT angiogram images, detecting an actionable LVO and alerting all parties through a mobile app. This removes the need for step-wise phone calls between multiple parties, repeating of the patient's history and logging in to review images at each step to make a decision. With these apps, all parties are simultaneously notified and can review images on the fly. The decision of whether

to proceed with EVT can be made within minutes of a patient being scanned.

I have had the fortune of having access to this capability during my one-year Health Manpower Development Plan training at the Gold Coast University hospital. With the app, I can even make transfer decisions for patients who are scanned in other peripheral non-EVT-capable hospitals within minutes of scanning, thus cutting out the multiple steps often required for the doctors in another hospital to eventually get in touch with me. Studies have shown that these apps have the potential to shorten the overall time to EVT treatment by at least 30 minutes, which translates to better clinical outcomes.<sup>2</sup>

## Back in Singapore...

However, I was quite dismayed to know upon my return to IT-savvy and AI-empowered Singapore, that the only “kosher” way for me to view a stroke patient’s imaging after hours and make the decision of whether to proceed with EVT is through the hospital-issued laptop. This is often a stressful affair because “time is brain” and it takes time to manoeuvre across the multiple layers of network access control: device posture check, log in, one-time password, app-specific log in and the occasional updates of virus definitions, which may take a good five to ten minutes. This is compounded by the fact that the stroke neurologist may sometimes have to struggle with these same steps before determining that it is an eligible EVT case and consulting me for my opinion. There are also occasions when I’m out running errands and the laptop is not readily available. Workarounds such as sending video clips of patient’s scans through the secure hospital messaging app from doctor to doctor are also quite suboptimal.

## Cybersecurity

In the wake of the SingHealth cyber attack in 2018, many policies and procedures were put in place to strengthen our IT defences and prevent such further attacks. These initiatives were probably put in place with the best of intentions from an IT professional’s point of view on how to safeguard the patient’s privacy and confidentiality rights with a very robust, almost impregnable security system.

One of the key strategies employed was to have internet separation, even though it adds a significant layer of inconveniences to our already hectic daily work. However, some of these measures also create significant challenges in integrating commercially available healthcare cloud-based/mobile/AI solutions such as the mobile stroke solution I highlighted above.

Perhaps we should re-examine the whole suite of our cybersecurity measures holistically from the perspective of the four fundamental principles of medical ethics. A patient’s rights to privacy and confidentiality are encapsulated under “Patient Autonomy” – the right of the patient to determine what he or she wants to let the caregiver to know (“privacy”) while confidentiality describes a situation whereby information disclosed is kept secret or “confidential” until the discloser (ie, the owner of this information) decides that more people can know about this information. Until then, the recipient of this information cannot divulge the information to anyone else. “Security” are measures that ensure the privacy and confidentiality rights of the patient or discloser are not compromised.

There are many other aspects to patient autonomy, including the right to accept and refuse treatment (informed consent, advance medical directive, etc). But the responsibilities of doctors and other healthcare professionals such as nurses do not end with patient autonomy, much less privacy, confidentiality and security. As a doctor, I must first do no harm (non-maleficence) and must do good (beneficence). This is what the patient came to the hospital or clinic for: that hopefully, I can do as much good as I can for the patient through my treatments and, at the same time, do as little harm as possible (there is always a harm, or at least the risk of harm element even in treatments – side effect of drugs, adverse events, complications, etc).

In the example I have described above for EVT, I find it extremely frustrating that I am unable to maximise my beneficence because of the primacy of security concerns. Security measures are put in place to ensure that privacy and confidentiality, subsets of patient

autonomy, are maintained. I hope that healthcare professionals, IT professionals and policymakers can sit together and discuss the best way forward. As in most things, trade-offs are needed between the need for healthcare professionals to maximise the good they do for patients and the primacy of security concerns of the IT professionals.

Creating solutions takes significant time and resources. I am confident that agencies such as Integrated Health Information Systems and our government agencies are working extremely hard on designing the architecture and framework to integrate such software through the government commercial or hospital cloud. These solutions take time. While our patients entrust us to protect their privacy, they also entrust us to employ every available tool and resource to provide the best care possible at the most critical time of their life.

Hospitals in the world have been trialling and adopting the above mobile solution even five years ago. We are behind the curve. What does it take to make this a reality? How can we shorten or streamline the adoption of these useful commercially available healthcare software? ♦

---

## References

1. Kunz WG, Hunink MG, Almekhlafi MA, et al. Public health and cost consequences of time delays to thrombectomy for acute ischemic stroke. *Neurology* 2020; 95:e2465-75.
2. Al-Kawaz M, Primiani C, Urrutia V, et al. Impact of RapidAI mobile application on treatment times in patients with large vessel occlusion. *J Neurointerv Surg* 2022; 14(3):233-6.

Dr Chia is a proud member of the inaugural class of 2011 from the Duke-NUS Medical School. He used to be an electrical engineer but is now more adapt and passionate about plumbing (fixing problems with vessels) and making a positive impact on patients.

