The EDITORS' MUSINGS

Dr Tina Tan

Editor

Dr Tan is a psychiatrist with the Better Life Psychological Medicine Clinic, and a visiting consultant at the Institute of Mental Health. She is also an alumnus of Duke-NUS Medical School. Between work and family life, she squeezes time out for her favourite pastimes – reading a good (fiction) book and writing.

As a visiting consultant at a public hospital, I recently found that my password was due for its quarterly change. I changed it as instructed (not that I had a choice since I couldn't log onto any system), but because I visit said hospital infrequently, I promptly forgot my password and had to call my friendly neighbourhood IT support team. "Why didn't I write it down?", one might ask – because I was taught never to leave my passwords around. It didn't help that passwords have many more requirements nowadays: minimum lengths, special characters, numbers and more.

I get why things are this way. This month's issue discusses healthcare cybersecurity, and our contributors have written on the importance of protecting our electronic systems and patient records, and the disastrous consequences when things go awry. The fact is that hackers will keep trying to hold our systems hostage and cripple us. Ultimately, our patients pay the price.

But what of the flip side? Articles by Dr David Yung and Dr Chia Ghim Song exemplify the struggle between protecting our systems and the hindrances caused. Perhaps this entire debate is best summed up by Dr Chia, zeroing in on the fundamentals of medical ethics and our responsibility to patients: "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."

I leave this with you, dear reader, while I try to remember my new password.

Dr Alex Wong

Guest Editor

Dr Wong is a private practitioner who talks too much. This occasionally leads him to write strange things, eat strange foods, travel to strange places and attend strange weddings/funerals that he doesn't necessarily always want to be at. He thinks this is fun and what life should be about.

"Data is a precious thing and will last longer than the systems themselves."

Tim Berners-Lee, the inventor of the World Wide Web, presciently declared that data – and by extension, the control, transfer and manipulation of it – would become the biggest issue of our time.

Big data promises a bold future in healthcare. Seamless information sharing between care providers, unprecedented research insights and, most compellingly, opportunities to train artificial intelligence (AI) to augment existing patient care.

Statistics demonstrate that the need is dire. As recently as 2013, the survival-to-discharge rate of cardiac collapse patients was higher in Las Vegas casinos than that of cardiac collapse patients in inpatient settings. Unwitnessed inpatient falls remain a multibillion-dollar worldwide problem despite improved nursing protocols. The issues that AI promises to resolve are legion and the future is now. Tan Tock Seng Hospital and Mount Elizabeth Novena Hospital now employ state-of-the-art fall prevention systems, and Integrated Health Information Systems has employed AI in bed management programmes and the diagnosis of eye diseases.

Yet, data is only useful if it's shared. Inevitably, the collection of healthcare data puts patient privacy at an unprecedented risk. Cybersecurity must improve, but recent events have shown us how vulnerable we are. Ironically, human foibles remain the most intractable and inevitable security flaw of any computer system.

Perhaps then, we also need to be more judicious in our collection of data. In our air-conditioned nation of ubiquitous closed-circuit television cameras, how should we calibrate our data collection? Hard questions lie ahead for both the programmer and policymaker alike. In the asking, may we learn to navigate our way through this golden age of big data. ◆