CYBERSECURITY A PERENNIAL CONCERN

Text by Dr Ng Chee Kwan

This issue of *SMA News* focuses on cybersecurity in healthcare. It has become commonplace for clinics' information technology (IT) systems to be connected to the Internet. Clinic management systems are often web-based, while access to patient clinical records and submission of claims to the Government and third-party administrators are often being done online. It is also necessary to be connected to the Internet if a doctor wishes to access patient data from the National Electronic Healthcare Record (NEHR) or contribute to the NEHR. The proposed Health Information Bill will in fact make it mandatory for all healthcare licensees to contribute to the NEHR, and hence Internet connection will become obligatory.

Unfortunately, the downside of being connected online is the risk of a cybersecurity breach. A prominent example of a healthcare cybersecurity breach occurred in 2018, when hackers infiltrated the computers of a public health institution and stole the personal particulars of 1.5 million patients. On another occasion in 2021, a ransomware attack on a private eye clinic affected the personal data and clinical information of nearly 73,500 patients. There are more instances of clinics suffering from ransomware attacks which may not have been publicised.

Such attacks not only result in the breach of patient privacy and heavy financial penalties imposed on the licensee, but they may also affect the operations of the clinic if patients' medical records are rendered inaccessible.

As doctors, we would like to primarily concentrate on the business and practice of medicine and focus on treating our patients. However, in addition to our clinical practice, we are obliged to implement safeguards to protect our medical records against accidental or unlawful loss and to protect our patients' data. As such, we should implement sufficient cybersecurity measures and policies to help protect our clinics' IT systems from criminals with malicious intentions. We should also arm ourselves with knowledge of the immediate actions to be taken should we experience a cybersecurity breach.

If contribution to the NEHR is to be made mandatory for healthcare providers, I hope the Ministry of Health will look into collaborating with vendors to provide pre-approved cybersecurity packages that will allow clinics to meet the required cybersecurity requirements at a reasonable cost. It would be even better if such costs could be covered by grants or subsidies.

Hopefully, the various articles in this issue will provide you with a better understanding of cybersecurity management, so you can review and improve your respective cybersecurity measures. We are also planning to conduct a webinar on cybersecurity in the coming months (see page 23). Do stay tuned for further updates. ◆

Dr Ng is a urologist in private practice and current President of the SMA. He has two teenage sons whom he hopes will grow much taller than him. He has probably collected too many watches for his own good.

> *"We should also arm ourselves with knowledge of the immediate actions to be taken should we experience a cybersecurity breach."*