CYBERSECURITY IMPLICATIONS on the Future of Healthcare

Text by Dr Num Tanthuwanit and Dr Joshua Koo

Traditional healthcare systems have come under increasing pressure from factors such as rising healthcare costs, rising demand with supply unable to keep up, a rapid rise in chronic diseases, and ageing populations. Shifts in reimbursement models are also adding pressure to the system, with payors across the globe moving towards value-based reimbursement models for healthcare, where claims are linked to patient outcomes, and providers are incentivised to adopt a risk-sharing model and reduce costs. Given that out-of-pocket (OOP) payor contribution has been decreasing (there has been a 3% to 6% reduction in OOP contribution observed for most Southeast Asian countries in the last five years), we foresee increasing pressure from payors for providers to manage costs.

Public systems are already moving towards value-based financing and away from reimbursements based on services provided. Singapore's Ministry of Health (MOH) has started to explore and adopt a capitation model (providing a fixed amount of money per person enrolled in a health plan per unit of time, whether or not the enrolled person seeks care) and "bundled payments", where funding is based on a patient's entire care for a given time period, even if it is across multiple healthcare settings or attendances. This is also enabled through a framework of having a single clinical team oversee the overall care and rehabilitation plan, pushing providers to collaborate and offer seamless care. **Sharing of clinical data securely in these cases will be important across multiple healthcare settings to ensure smooth transition of care.**

Rising patient consumerism has also contributed to a gradual shift in the model of care away from the traditional hospitals to more patient-centric ones where care is provided in the most appropriate and convenient setting, either in the community or at home. This requires increased deployment and utilisation of monitoring and communication technologies across care settings, which in turn needs to be integrated and interconnected to ensure continuity of care. The COVID-19 pandemic has seen an accelerated adoption of such digital technologies by patients, providers and regulators.

Where material interventions such as bypass surgery and knee replacement are required, we foresee an amalgamation of online and offline touchpoints to form a "hybrid model" of care delivery. In the hybrid care model, in-patient elements across the care pathway (eg, medication, treatment, pathology, diagnostics and imaging) will be integrated with virtual elements (eg, remote consultations, post-treatment care and condition monitoring), forming a cohesive care experience enabled by technology.

From the current landscape of stand-alone digital health service providers, the future is expected to evolve to an ecosystem-based model of care enabled by integrated platforms, allowing data to be shared among stakeholders. Hybrid models of online and offline solutions will come into prominence – wellness solutions and virtual care will be prime areas of focus. Building the hybrid model of healthcare will require an overhaul of existing workflows and systems. For example, appointment booking systems will need to be digitalised and data will have to be interoperable between primary care providers and specialists. Staff will need to be retrained and job scopes reviewed. Back-end systems will also need to be able to handle large amounts of data. Consequently, advanced encryption protocols and proper data management in data lakes or data warehouses will be important to prevent breaches.

Cybersecurity concerns

This increasing digitalisation and networking of various dimensions of healthcare systems entails risks related to technical failures impacting patient care, but more importantly, it entails risks in cybersecurity. Given the vast amount of clinical data that needs to be accessed by providers, payors and patients, we can expect certain cybersecurity concerns. These include ransomware attacks, cryptojacking, data breaches and leaks, malware, phishing, misinformation and even threats to the supply chain.

According to the World Economic Forum, COVID-19 has shown that the world is at great risk of disruption by pandemics, cyberattacks and environmental tipping points.[1] Consequently, we should prepare for a COVID-19-like global cyber pandemic that will spread faster and further than a biological virus, with an equal or greater economic impact.

Security experts warn that the health sector is seen as a particularly lucrative target by cybercriminals, with health records being worth up to ten times the value of other data such as banking details. There are ample recent examples of healthcare systems being interrupted or even shut down due to cyberattacks. The National Health Service (NHS) in the UK has been subjected to repeated attacks, the most damaging being in 2017 when it was brought to

a standstill for several days due to the WannaCry ransomware outbreak. This affected hospitals and GP surgeries across England and Scotland.[2] Although the NHS was not specifically targeted, the global cyberattack highlighted security vulnerabilities which resulted in the cancellation of thousands of appointments and operations, together with the frantic relocation of emergency patients from stricken emergency centres. Staff were also forced to revert to pen and paper and use their own mobile phones after the attack affected key systems, including telephones.

The US Department of Health and Human Services also tracks cyberattacks and breaches at healthcare providers. Their records show that in 2021, there were 618 unique breaches and attacks, affecting at least 500 people.[3] Cybersecurity experts say healthcare providers must devote more resources to preventing cybersecurity attacks, as having to deal with attacks can be far more expensive. Scripps Health said a cyberattack last year cost the system US$112 million in lost revenue, with the cost of a typical healthcare breach in the US averaging US$9.4 million in 2021.

And in Singapore, we all still remember the damaging attacks on SingHealth's IT system which compromised the personal details of over 1.5 million patients.

What organisations can do

In line with these challenges, Singapore has already established standards for data sharing. All public clinics and hospitals will be required to contribute to the National Electronic Health Record (NEHR). This is currently voluntary for private healthcare providers, but is soon to be become mandatory.[4]

In terms of cybersecurity, MOH advises that a complete, accurate and maintained inventory of the IT assets in the organisation will facilitate the implementation of optimal security controls.[5] The inventory should include a minimum of these data: Asset ID, Hostname, IP Address, Operating System, Assigned to (User) and Location. Furthermore, there are technical, process-oriented and social elements that can help counter cybersecurity threats.

Technical elements

Separate user accounts must be assigned to each user in an organisation. Multi-factor authentication should also be used, requiring users to submit at least two factors before gaining access. Security patches should be updated regularly as they add new security features and fix vulnerabilities. Protection is required against malware, which could steal sensitive patient data.

Cyber Perimeter Defence can secure any network connected to the Internet from hackers attempting to intrude into the network to steal or modify information. Audit logs should be kept as records to track the network's access history. This will be useful in the event of a cyberattack to help figure out the nature of the breach.

Process-oriented factors

Third-party software and hardware can expose the systems to threats, such as breaches or leaks of clinical data. Hence, careful vendor management and selection is important. Incident reporting of phishing, malware and other data breaches is also encouraged.

Social aspects

Finally, and most importantly, the organisation should create an intentional cybersecurity culture. IBM conducted a study into the cyber breaches that occurred among thousands of their customers in over 130 countries. One of the key findings was that human error was a major contributing cause in 95% of all breaches.[6] A healthy security culture prioritises training employees on information security, how to report incidents, when to ask for help, and whom to contact to work together toward incident resolution. This includes being familiar with password security issues, using trusted connections/sites and keeping informed on the latest developments in cybersecurity.

Conclusion

Over the past two years, healthcare organisations have had to adapt to many disruptions and changes in the way they treat patients. The rapid speed of change came with heavy costs and meant that many organisations neither prioritised nor involved cybersecurity in their decision-making process. As a result, new vulnerabilities arose that continue to threaten them today.

It is time for a new take on protecting the organisation: ensuring day-to-day resilience as well as a proactive, pragmatic and strategic approach that considers risk and security from the onset as new programs are implemented. Most importantly, elevating cybersecurity culture so that every staff member is aware and receives adequate training is the best defence that we can provide for our patients and organisation. ◆

References

1. David N. What the COVID-19 pandemic teaches us about cybersecurity – and how to prepare for the inevitable global cyberattack. In: World Economic Forum. Available at: https://bit.ly/3xKnwHj. Accessed 16 June 2022.

2. The NHS cyber attack. In: Acronis. Available at: https://bit.ly/3yeqi9a. Accessed 16 June 2022.

3. Southwick R. Cyberattacks in healthcare surged last year, and 2022 could be even worse. In: Chief Healthcare Executive. Available at: https://bit.ly/3Nj2GnS. Accessed 16 June 2022.

4. About NEHR. In: IHiS. Available at: https://bit.ly/3tZnCtw. Accessed 16 June 2022.

5. Ministry of Health. Healthcare Cybersecurity Essentials. August 2021. Available at: https://bit.ly/39Qxijc.

6. Why Human Error is #1 Cyber Security Threat to Businesses in 2021. In: The Hacker News. Available at: https://bit.ly/3ygJnaH.

Dr Num is a Partner at EY-Parthenon. He was formerly CEO of Bumrungrad Hospital, Thailand, and OMNI Hospitals, Indonesia. He obtained his MBBS from the University of Melbourne, is a Fellow of the Australasian Faculty of Rehabilitation Medicine, the Royal Australasian College of Physicians, and has a Masters in Management from Stanford Business School.

Dr Koo is a Manager at EY-Parthenon. He is part of the Strategy and Transactions team and was previously a GP in Singapore. He has also been involved in various healthcare roles, such as Medical Scientific Liaison in Rare Diseases, as well as in Inflammation and Immunology. He holds an MBA from Columbia University and graduated with an MBBS from NUS.