SAFE HEALTH:
Safety Includes Ensuring Cyber and Data Security in Your Healthcare Practices Too!

Text by Adj A/Prof Raymond Chua

In recent years, the healthcare sector has undergone rapid digitalisation, consequently intensifying cyber and data security risks. The Cyber Security Agency of Singapore (CSA) reported escalating cyber threats to the healthcare sector globally, with ransomware attacks increasing from 12% to 18% in 2023.[1] Singapore is not immune to these threats, with private clinics and institutions falling victim to cyberattacks in recent years. For instance, a specialist medical clinic was targeted by a ransomware attack in August 2021. The incident affected its clinic server and management system, which contained data for over 73,000 patients. Fortunately, no clinical services were disrupted by this cyberattack.

Such incidents underscore the urgent need for robust cybersecurity measures in healthcare, as exemplified by cases like the National Health Service (NHS) England attack in June 2024, which demonstrated the potential impact of cyberattacks on patient care and safety.[2] This incident was a significant cyber-attack that targeted London's NHS hospitals, specifically affecting pathology services at Guy's and St Thomas' and King's College Hospital NHS Foundation Trusts. This ransomware attack, reportedly linked to Russian cybercriminals, disrupted critical medical operations by impairing Synnovis, a key pathology provider responsible for processing blood tests across multiple NHS sites in London. The incident led to the cancellation of over 800 surgeries and 700 outpatient appointments, and forced the destruction of thousands of blood samples due to service limitations.

Recognising these emerging threats, the Ministry of Health (MOH) issued the Healthcare Cybersecurity Essentials (HCSE) in 2021 to provide guidance on baseline cyber hygiene and introduced cybersecurity requirements for clinical management systems. The HCSE was further enhanced in December 2023 into the Cyber and Data Security Guidelines, providing an overview of what enforceable standards under the upcoming Health Information Bill (HIB) might entail, giving healthcare providers time to familiarise themselves with the steps needed to uplift their cyber and data security posture for their systems, practices and people prior to promulgation of the Bill sometime in early 2025. For more information on the Cyber and Data Security Guidelines and for further details on the HIB, please refer to https://healthinfo.gov.sg.

Connected medical devices and CLS (MD)

In addition, the use of connected medical devices has been increasing, fuelled by changing care delivery models to shift more care into the community and allowing remote monitoring of patients. Hence, cybersecurity in medical devices becomes even more crucial as these devices are now vulnerable to cyber threats, such as unauthorised access to sensitive patient data, or worse, manipulation of device settings

to impact patient care. To address these concerns, MOH, in collaboration with CSA, the Health Sciences Authority and Synapxe, launched a Cybersecurity Labelling Scheme for Medical Devices (CLS [MD]) in October 2024, with the aim of raising cyber hygiene levels in medical devices. More details on CLS (MD) can be found at https://bit.ly/3Yu56I8.

Your SAFE HEALTH tips

To make it easier for healthcare providers and professionals to remember and apply cybersecurity concepts effectively, I distil below ten tips to summarise the key points from the Cyber and Data Security Guidelines, easily remembered as **SAFE HEALTH**.

S – Secure and protect

- Use anti-malware and anti-virus solutions to protect against malicious software.
- Use secure settings for your organisation's procured hardware and software.
- Consider using medical devices assessed under CLS (MD).

A – Asset

- Identify and protect all hardware and software assets used in your organisation.
- Identify the types of data your organisation has, where they are stored and secure them.

F – Frequent updates

- Regularly update software and systems to prevent vulnerabilities.
- Install software updates on your devices and systems promptly.

E – Emergency planning and incident response

- Create and test an emergency plan to ensure business continuity during service disruptions.
- Be prepared to detect, respond to and recover from incidents.

H – Harness backups

- Perform regular backups of essential data and store them securely offline (eg, disconnected physical media).

E – Evaluate and audit

- Conduct audits and regular security reviews to identify and address vulnerabilities.
- Review corporate policies and processes to ensure compliance.

A – Authorised users

- Implement access control measures to control individual access to your data and services.
- Restrict access to health information for valid and relevant purposes.

L – Labelling and data security classification

- Know the information sensitivity levels of the data to apply appropriate safeguards.
- Differentiate data of varying information sensitivity levels by marking their classification.

T – Train staff

- Equip staff with cyber hygiene practices and to securely store health information to prevent unauthorised access.
- Educate on the proper conveyance and reproduction of health information to avoid unwanted data exposure.

H – Handle outsourcing and disposal

- Understand and define the responsibilities between your organisation and vendors.
- Implement proper disposal procedures for health information to mitigate the risk of unauthorised access.

By following these tips, healthcare providers and professionals can significantly enhance their cyber and data security posture to protect patient data, ensuring the continuity of safe and efficient care. Remember that safeguarding data and upkeeping cybersecurity are ongoing processes that require constant vigilance and adaptation to new threats. Stay proactive and informed to safeguard patient data and maintain trust in your organisation.

Following the promulgation of the Bill, MOH will be reaching out to provide additional support and training tips. Keep an eye out for further updates in 2025!

For queries or feedback, please email HIA_Enquiries@moh.gov.sg. ◆

References

1. Cyber Security Agency of Singapore. Singapore Cyber Landscape 2023. Singapore: Cyber Security Agency of Singapore, 2024.

2. Evans H, Thomas R. Data from NHS cyber attack that cancelled operations 'published online by criminal group'. The Independent [Internet]. 21 June 2024. Available at: https://bit.ly/4eiiWmR.

Adj A/Prof Chua is the Chief Executive Officer-Designate of the Health Sciences Authority responsible for safeguarding and advancing public health through securing the national blood supply, administering national justice through its forensic medicine and scientific testing capabilities and regulating the health products. He is also the Deputy Director-General of Health (Health Regulation) at the Ministry of Health overseeing the regulation of healthcare services and information.