

# Summary of Key Events: 7

- The public announcement was made on 20 July 2018, and patient outreach and communications commenced immediately thereafter.
- SMS messages were used as the primary mode of communication, in view of the need for quick dissemination of information on a large scale.
- **COI Committee has identified 5 key Findings!**

## KEY FINDING 1

- IHiS staff did not have adequate levels of cybersecurity awareness, training, and resources
  - to appreciate the security implications of their findings and
  - to respond effectively to the attack.

## KEY FINDING 2

- **Certain IHiS staff** holding key roles in IT security incident response and reporting
  - **failed to take appropriate, effective, or timely action**, resulting in missed opportunities to prevent the stealing and exfiltrating of data in the attack

## KEY FINDING 3

There were a **number of vulnerabilities, weaknesses, and misconfigurations** in the SingHealth network and SCM system that **contributed to the attacker's success** in obtaining and exfiltrating the data, **many** of which **could have been remedied** before the attack

## KEY FINDING 4

**The attacker was a skilled and sophisticated actor bearing the characteristics of an Advanced Persistent Threat group**