



Singapore's HIV Registry Data Breach: What Can We Learn?

On 28 January 2019, the Singapore Ministry of Health (MoH) was alerted by the Singapore Police that confidential information regarding 14,200 individuals diagnosed with HIV had been leaked online.

What was stolen?

The data included names, identification numbers, contact details, and critically, the HIV positive status of these individuals and their related medical information. The medical records belonged to 5,400 Singaporeans diagnosed with HIV since 1985 up to January 2013, as well as 8,800 foreigners diagnosed with HIV up to December 2011.

How did it happen?

The perpetrator was a foreigner who resided in Singapore from 2008 to 2018. He allegedly acquired the information through his partner, the former head of Singapore's National Public Health Unit, who had authority to access information in the HIV Registry.

In 2016, MoH received information that an unauthorised person was in possession of confidential information that appeared to be from the HIV Registry. His property was searched, and all relevant material found was seized and secured by the Police.

In May 2018, after the perpetrator was deported from Singapore (after being jailed for non-related offenses), MoH received information that he still had part of the records he held in 2016. While the information did not appear to have been disclosed in any public manner, MoH began notifying the affected individuals.

On 22 January 2019, MoH was notified that the information had been leaked online.

We're here to
empower results

To find out how Aon can
enhance your cyber resilience,
please contact:

Murray Wood

Head of Financial Specialties, Asia
+65 6645 0116
murray.wood@aon.com

Andrew Mahony

Regional Director, Financial Services
& Professions Group
+65 6313 7080
andrew.mahony@aon.com

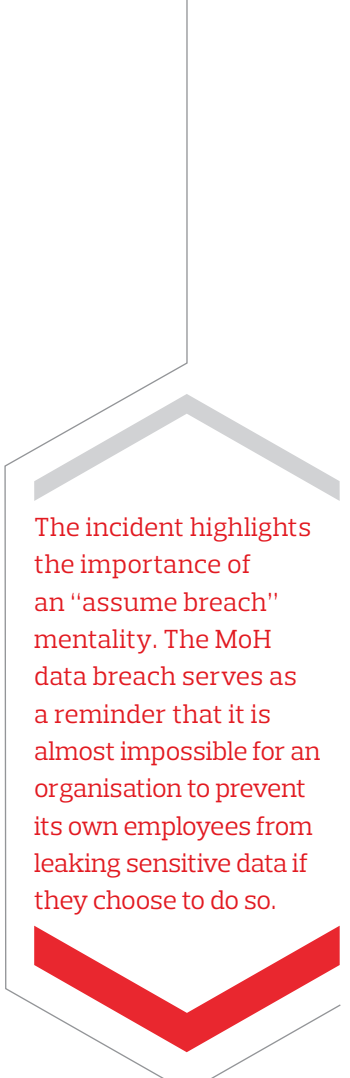
What now?

MoH continues to contact the affected parties. A hotline has been set up for those affected, and counselling will be offered.

Since 2016, additional safeguards against mishandling of information by authorised staff have been put in place around Disease Registries, including a two-factor authentication requirement when accessing sensitive data.

What can organisations like yours take from this incident?

- Data breaches can arise from outside and within. Last year's SingHealth data breach demonstrated the danger that sophisticated external forces can pose. This year's breach arose from a compromised individual within the Ministry of Health.
- Healthcare data continues to be at risk. Motivations vary: historically, they have been commercial, given the high value healthcare records can fetch on the dark web. In the SingHealth breach, the suspected motive was geopolitical; and in this breach, the motivation appeared to be personal.
- Internal controls on data privacy and security are necessary. The MoH has acknowledged that security has been tightened since the initial breach, with two-factor authentication now required to access sensitive data. Monitoring of how that data travels, particularly outside of the company's systems, is critical.
- The incident highlights the importance of an "assume breach" mentality. While this phrase is commonly used to express the likelihood that an external hacker can access a company's system, the MoH data breach serves as a reminder that it is almost impossible for an organisation to prevent its own employees from leaking sensitive data if they choose to do so. In addition to tightening controls on access and data exfiltration, companies should prepare to respond to breaches of this nature, by drafting and testing incident response plans, engaging incident response providers pre-breach and investing in cyber insurance.



The incident highlights the importance of an "assume breach" mentality. The MoH data breach serves as a reminder that it is almost impossible for an organisation to prevent its own employees from leaking sensitive data if they choose to do so.

How can Aon help?

Aon Cyber Solutions offers a wide range of services to support your company's cyber resilience:

- **Internal Investigations**

When an organisation suspects that an employee or ex-employee has acted inappropriately (accessing sensitive data, copying intellectual property, breaching covenants etc.), the Aon Cyber Solutions team has the forensics, investigation, and evidence handling experience to help internal legal, audit, IT, and compliance teams, especially where legal action may result.

We apply our unique, industry-leading tool sets to trace data access and movement and provide clear guidance on the findings to the client.

- **Cyber Insurance**

In responding to a breach of this nature, likely expenses include:



- a) **Forensic investigation costs**
- b) **Legal advice**
- c) **Public relations consultancy; and**
- d) **Notification costs.**

A company in these circumstances may also be exposed to third-party liability and regulatory investigation expenses. All of these exposures can be covered with a cyber insurance policy.

Aon has experience in placing robust and bespoke cyber insurance policies for some of Asia's largest companies and can work with your organisation to design an appropriate cyber risk transfer strategy.

- **Incident Response**

The Aon Cyber Solutions team comprises go-to experts for organisations and their law firms in investigating 90 percent of the highest profile breaches in the last decade. We are global leaders in incident response, digital forensics, eDiscovery, investigations, and security advisory. Our team of seasoned professionals is equipped to help you defend an attack, recover from an incident, secure your systems, minimise business interruption, and recuperate losses, while preserving evidence and confidently communicating with your stakeholders.

The Aon Cyber Solutions team comprises go-to experts for organisations and their law firms in investigating 90 percent of the highest profile breaches in the last decade. We are global leaders in incident response, digital forensics, eDiscovery, investigations, and security advisory.