COMMISSIONER FOR PERSONAL DATA PROTECTION

[2019] SGPDPC 3

Case No DP-1807-B2435

In the matter of an investigation under section 50(1) of the Personal Data Protection Act 2012

And

(1) Singapore Health Services Pte. Ltd. (UEN No. 200002698Z)

(2) Integrated Health Information Systems Pte. Ltd. (UEN No. 200814464H)

… *Organisations*

DECISION

Singapore Health Services Pte. Ltd. & Ors.

[2019] SGPDPC 3

Tan Kiat How, Commissioner — Case No DP-1807-B2435

14 January 2019

1 This case concerns the worst breach of personal data in Singapore's history. In an unprecedented cyber attack on the Singapore Health Services Pte Ltd's ("**SingHealth**") patient database system, the personal data of some 1.5 million patients and the outpatient prescription records of nearly 160,000 patients were exfiltrated in a cyber attack (the "**Data Breach**").

2 Following the announcement on 20 July 2018 by the Ministry of Communications and Information and the Ministry of Health ("**MOH**"), a four-member Committee of Inquiry ("**COI**") was convened by the Minister for Communications and Information to look into the cyber attack, find out what went wrong and recommend ways to better safeguard critical systems. The COI concluded its hearings and submitted its report on 31 December 2018 to the Minister-in-charge of Cyber Security. The public report of the COI's findings was released on 10 January 2019 ("**Public COI Report**").

3 Soon after the announcement of the Data Breach, the Personal Data Protection Commission (the "**Commission**") received several complaints from members of the public regarding the Data Breach. The Commission commenced its investigations thereafter ("**Investigation**"). The organisations involved were SingHealth and Integrated Health Information Systems Pte Ltd ("**IHiS**").

4 SingHealth and IHiS (collectively, the "**Organisations**") agreed to cooperate with the Commission to expedite the Investigation and determination of liability and for the Commission to issue such directions that it deems fit on the basis of the Organisations' representations. In this regard, the Organisations voluntarily and unequivocally admitted to the facts as set out in this Decision and accepted the Commissioner's findings in this Decision.

5 The Commissioner's findings and grounds of decision, which are based on the Organisations' representations, are set out below. Additionally, the Organisations have agreed to incorporate references to relevant sections of the Public COI Report relating to their

representations and the factual issues addressed therein. Accordingly, the Commissioner has referred to some parts of the Public COI Report in the grounds of decision.

Material Facts

6 The following chronology and summary of admitted facts were provided by IHiS and SingHealth in its submissions. SingHealth is one of three healthcare clusters in the Singapore public healthcare sector. In Singapore, public healthcare institutions ("**PHIs**") are grouped into clusters ("**Clusters**"). IHiS and SingHealth are wholly-owned subsidiaries of MOH Holdings Pte Ltd ("**MOHH**"), the holding company through which the Singapore government owns the corporatised institutions in the public healthcare sector. MOH determines the policies and structures within the healthcare sector.

7 The SingHealth Cluster comprises Singapore General Hospital ("**SGH**"), Changi General Hospital, Sengkang General Hospital, KK Women's and Children's Hospital, National Cancer Centre, National Dental Centre Singapore, National Heart Centre Singapore, National Neuroscience Institute, Singapore National Eye Centre, SingHealth Community Hospitals and SingHealth Polyclinics.[1] SingHealth's primary function is the provision of healthcare services.

8 IHiS is the central national IT agency for the public healthcare sector in Singapore. IHiS is also the MOH-designated Sector Lead for the healthcare sector for liaising with the Cyber Security Agency of Singapore ("**CSA**"). Prior to 2008, PHIs were responsible for their own IT functions and strategy. In July 2008, IHiS was established by MOH to centralise all of the IT functions and capabilities of the PHIs (including IT staff) in a single entity, which would support all the PHIs. IHiS also assumed responsibility for the development and maintenance of the Clusters' IT systems (including SingHealth). The objectives of centralisation were to, *inter alia*: (i) enable better alignment of IT strategies and integration of patient care across PHIs, and (ii) reduce the cybersecurity vulnerabilities inherent in a varied and fragmented IT landscape.

9 IT resources in the public healthcare sector were further consolidated in November 2016, when MOHH's Information Systems Division ("**ISD**") was merged into IHiS. With this merger, national healthcare systems which were originally managed by ISD came under IHiS'

[1] Polyclinics in Bedok, Bukit Merah, Marine Parade, Outram, Pasir Ris, Punggol, Sengkang and Tampines, as well as Bright Vision Hospital. Two other polyclinics in Queenstown and Geylang used to be under SingHealth.

management as well. Each Cluster, SingHealth not excepted, has a Group Chief Information Officer ("**GCIO**") and a Cluster Information Security Officer ("**CISO**"). Pursuant to the public healthcare sector policy, Healthcare IT Security Policy and Standards (Version 3.0) ("**IT-SPS**"), the GCIO provides leadership and direction for the Cluster's IT security program, including the establishment and maintenance of the program objectives, strategy, and near- and medium-term activities such as aligning strategic IT initiatives with the Cluster's business objectives. The GCIO is assisted by the CISO, who is charged with security oversight for the Cluster. The CISO reports to the GCIO directly on security matters.

10 Upon the formation of IHiS in 2008, the employment of the majority of IT staff across the Clusters at the time, including SingHealth, were transferred to IHiS. Since then, IHiS has been responsible for hiring and managing IT personnel at both the management and operational level for functions such as general management, maintenance and security management. However, IHiS designates some IT personnel to be redeployed to the Clusters to be responsible for providing leadership and direction for the IT security program as well as executive management oversight of the local Cluster IT systems. In the present case, the SingHealth GCIO and SingHealth CISO are employed by IHiS but deployed to SingHealth to serve the IT needs of SingHealth. The staff of the SingHealth GCIO Office[2] that supports the SingHealth GCIO and carries out, among other duties, operational and security oversight of SingHealth's IT systems are also deployed by IHiS to SingHealth.[3]

11 GCIOs are accountable to their Clusters for the Chief Information Officer ("**CIO**") services they provide, such as IT capability development, systems resiliency and security. In SingHealth, the GCIO reports to SingHealth management via the SingHealth Deputy Group Chief Executive Officer (Organisational Transformation and Informatics) ("**DGCEO (OT&I)**"). The SingHealth GCIO is also concurrently accountable to the Chief Executive Officer ("**CEO**") of IHiS for the quality of the CIO services provided to the Cluster.[4]

12 IHiS has a centralised Delivery Group which manages the day-to-day operations and technical support, maintenance and monitoring of the entire SingHealth IT system, including

[2] The SingHealth GCIO Office has a staff strength of 50 members who are IHiS employees.
[3] The SingHealth GCIO Office is made up of staff deployed from IHiS who are mostly IT Directors from SingHealth's institutions that carry out management oversight roles of the institutions' IT operations.
[4] The CEO of IHiS sets the key performance indicators of the SingHealth GCIO and GCIO Office, namely capability development, resiliency and cost effectiveness.

the Sunrise Clinical Manager system ("**SCM**"), as well as the other Clusters' IT systems. The IHiS Delivery Group also covers the security aspects of the Clusters' IT systems and plays a supportive role in rolling out security measures. Within the IHiS Delivery Group, the Security Management Department ("**SMD**") covers a broad portfolio of IT security in the Clusters. The SingHealth GCIO Office relies on the IHiS Delivery Group for their technical expertise on security and operational matters.

SingHealth's Electronic Medical Record system

13 SingHealth uses SCM, an Electronic Medical Record ("**EMR**") software solution from Allscripts Healthcare Solutions, Inc ("**Allscripts**"). Through SCM, there is a single enterprise-wide EMR containing real-time patient data. SCM is vital to SingHealth's operations and is actively used by SingHealth staff in patient care and management.

14 SCM was implemented by SingHealth in 1999. The IHiS Delivery Group took over the management of SCM in 2008, when the IT team at SingHealth responsible for managing SCM was transferred to IHiS. The SCM database contains patient medical records, including the following types of personal data concerning SingHealth's patients:

(a) patient particulars (e.g. name, National Registration Identification Card numbers ("**NRIC**"), address, gender, race and date of birth);

(b) clinical episode information (e.g. A&E, inpatient, outpatient);

(c) orders (e.g. laboratory, radiology, cardiology, medication, nursing);

(d) results (e.g. of diagnostic tests and orders);

(e) clinical documentation (e.g. from doctors, nurses, rehabilitation);

(f) vital signs (e.g. blood pressure, pulse);

(g) medical alerts and allergies;

(h) diagnosis and health issues;

(i) vaccination details;

(j) discharge summaries;

(k) medical certificates; and

(l) outpatient medication dispensed (with associated patient demographics).

15 As of July 2018, the SCM database contained patient data of over 5.01 million unique individuals.

16 The SCM IT network is spread across two sectors:

(a) the SingHealth network, which includes infrastructure in the SingHealth campus; and

(b) the Healthcare-Cloud ("**H-Cloud**") at the Healthcare Data Centre ("**HDC**"). H-Cloud was set up in 2014 by IHiS as part of a data centre consolidation exercise across the PHIs as well as for IHiS to leverage cloud technologies in serving the PHIs.

17 Before June 2017, the SCM system (which includes the Citrix servers hosting the SCM client application and the SCM database servers) was located at SingHealth's SGH campus. The Citrix servers serve as middleware (i.e. the bridging between an operating system or database and applications on a network) supporting many applications used in SingHealth's daily operations, including the SCM client application. Citrix servers allow for virtualisation of the SCM client application without the need for a local installation on the user's workstation. There is no transactional data that flows directly between the user's workstation and the SCM database. Users can only view screen images of the SCM client application.

18 The SCM system at SGH (i.e. both the SCM database servers and Citrix servers) was migrated to be hosted in H-Cloud in June 2017. Since June 2017, a typical SingHealth user would access the SCM system in the following manner:

(a) from the user's workstation, the user launches a virtual SCM client application hosted on the H-Cloud Citrix servers. The application will require the user to enter his unique user credentials to log in to the SCM client application. The user credentials are sent through the Citrix server to the SCM security server for authentication; and

(b) upon successful authentication, the user will be able to access information on the SCM database corresponding to the user's designated role and responsibilities.

Data Breach

19 Between 27 June to 4 July 2018, the personal data of 1,495,364 unique individuals were illegally accessed and copied from the SCM database. The illegal access and copying was limited to a portion of the SCM database, and only in respect of the following personal data:

(a) the names, NRIC numbers, addresses, gender, race, and dates of birth ("**Patient Particulars**") of 1,495,364 SingHealth patients; and

(b) the outpatient dispensed medication records ("**Dispensed Medication Records**") of 159,000 patients (which is a subset of the full set of illegally accessed personal data).

Sequence of events

20 Based on forensic investigations by IHiS and CSA, the attacker gained initial access to the SCM network in August 2017 by infecting a user's workstation. This was likely through an email phishing attack, which led to malware and hacking tools subsequently being installed and executed on the user's workstation.

21 Once the attacker established an initial foothold through the affected workstation, the attacker used customised malware to infect and subsequently gain remote access to and control of other workstations between December 2017 and May 2018. From these compromised workstations, the attacker was able to gain access to and control of two user accounts: (i) a local administrator account, and (ii) another service account (a special user account that applications or services use to interact with the operating system) ("**Compromised Accounts**"):

(a) the local administrator account was a dormant account not ordinarily used for day-to-day operations, and was originally created as a back-up account for use by administrators. This account was secured with an easily deduced password ("P@ssw0rd"); and

(b) the service account was also a dormant account with full administrative privileges. This account was secured with a password which was self-generated during the installation of the services.

22 Through these Compromised Accounts, the attacker was able to gain access to and control of the Citrix servers located at SGH ("**SGH Citrix Servers**"). IHiS had planned to decommission these SGH Citrix servers following the migration of the SCM database and the Citrix servers to H-Cloud in June 2017 but the SGH Citrix Servers remained operational and part of the SCM network while the decommissioning process was ongoing because the SGH Citrix Servers were still hosting other applications which were either planned for migration to H-Cloud or decommissioning by FY 2018.

23 While the attacker had managed to log in to the SGH Citrix Servers, which gave it a direct route to the SCM database, the attacker still did not have the credentials that would have enabled it to log in to the SCM database. As such, between end-May to mid-June 2018, the attacker made multiple failed attempts to access the SCM database using invalid credentials, or accounts that had insufficient privileges to gain access to the SCM database.

24 On 11 June 2018, an IHiS database administrator from the IHiS Delivery Group discovered the multiple failed attempts to log in to the SCM database. She noticed that some user IDs were used on separate occasions to log in to the SCM database, but they could not log in because they were non-existent user IDs or were not granted access. One of the user IDs belonged to a domain administrator from the IHiS Systems Management Department but she verified that he had not made any attempts to log into the database.

25 More attempts to log in to the database were made on 12 and 13 June 2018. One of the user IDs used was the same as those used on 11 June 2018. It became clear to her on 13 June 2018 that the failed attempts to log in were evidence of someone attempting to gain unauthorised access to the database. On 13 June 2018, a few members of the staff from the IHiS Delivery Group met with the SMD over these login attempts. A chat group was created; members included the SIRM, the SingHealth CISO and members of the SMD.

26 On 26 June 2018, the attacker managed to obtain login credentials for the SCM database from the H-Cloud Citrix server. CSA assessed that there was an inherent coding vulnerability in the SCM client application which allowed the attacker to retrieve the SCM database login credentials from the H-Cloud Citrix server. These credentials were then used to access the SCM database using one of the compromised SGH Citrix Servers.

27 Between 27 June and 4 July 2018, the attacker used the stolen SCM database login credentials to access and run numerous bulk queries from one of the compromised SGH Citrix Servers on the SCM database. Data that was illegally accessed and copied through such queries was then exfiltrated by the attacker through the initial compromised workstations to the attacker's overseas Command and Control ("**C2**") servers.

28 Suspicious circumstances were observed by staff of the IHiS Delivery Group who were not members of the SMD. They brought their suspicion to the attention of individual personnel from IHiS' Security Incident Response Team ("**SIRT**"), which is part of the SMD. One of the personnel thus notified was the Security Incident Response Manager ("**SIRM**"). The staff in the IHiS Delivery Group had reported the suspicious circumstances as they suspected that there was something amiss. While the matter was referred to the SMD, the SIRT was not formally activated at any point. This was not in accordance with IHiS' Healthcare IT Security Incident Response Framework, version 2.1 ("**SIRF**") and IHiS' Cluster IT Security Incident Response SOP, version 1.0 ("**IR-SOP**").

29 On 4 July 2018, an IHiS Assistant Lead Analyst from the IHiS Delivery Group supporting SCM observed alerts generated by a performance monitor which was programmed to monitor database queries. He commenced investigations into the unusual queries on the SCM database. When the Assistant Lead Analyst was unable to trace the user launching the queries or make sense of the queries on his own, he alerted his colleagues from the IHiS Application, Citrix and Database teams to assist in the investigations. An automated script was then developed and implemented on the SCM database by the Assistant Lead Analyst together with an IHiS Database Administrator from the IHiS Delivery Group to terminate the queries, log the queries and send alerts to them when such queries are identified. The Citrix Team Lead also took steps to block access to the SCM database from any SGH Citrix Server, and submitted requests to create firewall rules to block all connections to the SCM database originating from any SGH Citrix Server. Collectively, these efforts stopped the further exfiltration of data from the SCM database.

30 The SIRM and the SingHealth CISO were both aware of the suspicion of attack since 13 June 2018 and the remediation efforts of 4 July 2018. They were both copied on emails and were members of a chatgroup created to investigate these incidents. The SingHealth CISO was apprised of the investigations but did not make further enquiries. Instead, he waited passively

for updates. The SIRM was overseas until 18 June 2018 without nominating a covering officer. During this time, neither the SIRM nor the SingHealth CISO escalated the matter despite their knowledge of these circumstances through meetings and messages. Also, neither the SIRM nor the SingHealth CISO took any steps to activate the SIRT in accordance with the IR-SOP.

31 IHiS senior management and the SingHealth GCIO were only alerted to the attack on the evening of 9 July 2018. Even though the SingHealth GCIO did not receive details of the unauthorised access (and in particular the exfiltration of data), he promptly escalated the matter and informed the CEO of IHiS that there was suspected unauthorised access into the SCM database. Concurrently, the SingHealth GCIO informed the SingHealth DGCEO (OT&I) of the suspected unauthorised access. After being informed, the CEO of IHiS consulted with IHiS' director for Cyber Security Governance ("**CSG**") and organised an urgent conference call between IHiS senior management and the relevant employees at 1:00 p.m. the next day, where he was to be briefed on the matter.

32 Details of the attack and the exfiltration of data were first shared with the CEO of IHiS and the SingHealth GCIO, at the conference call on 10 July 2018. The CEO of IHiS immediately recalled all relevant employees and IHiS senior management for an urgent meeting at IHiS' office on the matter and to undertake an examination of IHiS' logs of the attacker's queries on the SCM database to ascertain the extent of data exfiltration (if any). More details of the incident were ascertained and the CEO of IHiS and IHiS senior management were informed of the same at the meeting that afternoon. Arrangements were made to immediately notify CSA. Notifications were also issued by IHiS to MOH and SingHealth. A "war room" with five working cells for containment, investigation, patient impact, communications and reviewing of security measures for other systems was also set up.

Remedial actions

33 From 10 July 2018, IHiS and CSA worked jointly to put in place containment measures to isolate the immediate threat, eliminate the attacker's foothold and prevent the attack from recurring:

(a) IHiS reset the system accounts twice in succession to invalidate any existing full-access authentication tokens that the attacker might have;

(b) IHiS Security Operations Centre was placed on high alert to look out for suspicious activity and signs of compromise and failed login attempts, which allowed CSA and IHiS to detect and respond to fresh callback attempts by the attacker on 19 July 2018 to the C2 servers;

(c) the IHiS Network team tightened firewall rules;

(d) IHiS reloaded all Citrix servers with clean images to ensure no compromised Citrix servers were left running;

(e) IHiS mandated passwords changes for all users (including administrators); and

(f) IHiS put in place extensive monitoring of all administrator accounts.

34 IHiS also supported CSA in its investigations by providing forensic images of computers suspected to be compromised, memory dumps, and proxy and network logs for forensic analysis by CSA. IHiS also simulated the attacker's queries to ascertain the extent of data exfiltration.

35 On 19 July 2018, attempts by the attacker to access the SCM network were again detected and CSA recommended the adoption of Internet Surfing Separation ("**ISS**") to contain the attack. ISS was instituted immediately thereafter on 20 July 2018 for SingHealth, and by 22 July 2018 for the other two Clusters.

36 Shortly after SingHealth was informed of the cyber attack, SingHealth made plans for patient communications using multiple channels of communication. Within days after the public announcement of the cyber attack on 20 July 2018, SingHealth sent out SMSes or letters to notify patients whether their data was illegally accessed and how they can seek help. Telephone hotlines were also set up for members of the public to obtain further information. Members of the public could also check whether their data had been accessed on the "HealthBuddy" mobile application and the SingHealth website.

37 On 1 November 2018, IHiS announced that it will be adopting a slew of measures to strengthen cybersecurity across the public healthcare sector following the cyber attack. IHiS identified and initiated 18 security measures which will be implemented progressively. Such measures include:

(a) addressing Advanced Persistent Threat ("**APT**") by sophisticated actors: IHiS has initiated several measures to improve its ability to detect indicators-of-compromise, record and monitor endpoints' system-level behaviours and events, detect advanced malwares and remove the threats (if any). IHiS will also be implementing two-factor authentication for endpoint local administrators who manage end-user devices and installation of software;

(b) addressing vulnerabilities to prevent unauthorised access to Clusters' IT networks: To further prevent the use of weak passwords, IHiS will be enhancing the access management capability to manage complex passwords centrally and automatically update and protect administrator accounts. Access management will be boosted with threat analytics to provide earlier detection of suspicious account activities by applying a combination of statistical modelling, machine learning, as well as behaviour analytics to identify unusual activities, and respond faster to threats; and

(c) enhancing security of the Allscripts SCM: IHiS has put in place database activity monitoring for SCM and it is being enhanced with more comprehensive blocks and alerts on execution of bulk queries.

Findings and Basis for Determination

38 The issues for determination are as follows:

(a) whether IHiS was acting as a data intermediary for SingHealth in relation to the SingHealth patients' personal data on the SCM database; and

(b) whether each of the Organisations complied with its obligation under section 24 of the Personal Data Protection Act 2012 ("**PDPA**") in respect of the Data Breach.

39 As a preliminary point, the Commissioner finds that the Patient Particulars and Dispensed Medication Records are personal data as defined under section 2(1) of the PDPA because they contain data about patients who could be identified from that data.

40 Given the facts and circumstances surrounding the Data Breach, the Patient Particulars and Dispensed Medication Records were disclosed without authorisation in the Data Breach.

(a) Whether IHiS was acting as a data intermediary for SingHealth

41 A data intermediary is defined in section 2(1) of the PDPA as an organisation that processes personal data on behalf of another organisation but does not include an employee of that organisation. SingHealth engaged IHiS (MOH's designated IT arm of the public healthcare sector), as required by MOH, to manage its IT systems and provide day-to-day operations and technical support, maintenance, and monitoring of the entire SingHealth IT system (including the SCM database which held the personal data of SingHealth's patients). These activities include "processing" of personal data on behalf of SingHealth, as defined in section 2(1) of the PDPA.

42 The scope of the IHiS Delivery Group's duties and responsibilities to SingHealth are set out in the following policy documents:

(a) the IT-SPS, which is a policy document jointly prepared by MOHH and IHiS;

(b) the annual IT workplans for each of the SingHealth institutions, which establish an agreement between each of the SingHealth institutions and IHiS;[5] and

(c) the IHiS Data Protection Policy ("**DPP**") (read in conjunction with the MOHH Information Sharing Policy), which expressly states that IHiS is a data intermediary for SingHealth and all other healthcare institutions in the Clusters.[6]

43 Notably, the DPP makes it clear that IHiS will only collect, use, disclose and/or process SingHealth's data to the extent necessary to fulfil its duties and obligations to SingHealth. This includes, among other things, collecting, using, disclosing and/or processing SingHealth's data for the purposes of investigating and resolution of issues and errors reported in IT programs and systems and IT support.[7]

---

[5] The IT workplans expressly include the provision of SCM maintenance support as an item under the list of "IT System Support and Maintenance Services" to be provided.

[6] Clause 1.1.3 of the DPP states:

> "As IT professionals who support healthcare organisations, **IHIS acts as a "data intermediary" in relation to Client Data, will exercise reasonable care in protecting Client Data** from unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks (our "**Protection Obligation**"), and we **undertake steps to ensure that we do not retain personal data longer than is required for business or legal purposes** (our "**Retention Obligation**").
>
> [Emphasis added.]

[7] Clause 6.1.1 of the DPP.

44 Pursuant to section 4(2) of the PDPA, a data intermediary that processes personal data on behalf of and for the purposes of another organisation pursuant to a contract which is evidenced or made in writing has a duty to comply with sections 24 and 25 of the PDPA. Under section 4(3) of the PDPA, an organisation that engages a data intermediary to process personal data on its behalf and for its purposes has the same obligation in respect of such personal data as if it had processed the personal data itself. Accordingly, SingHealth and IHiS each have an obligation to make reasonable security arrangements to protect the personal data of SingHealth's patients that are in their possession or under their control.

The GCIO Office

45 At this juncture, it is pertinent to deal with the issue of where the roles of the GCIO (and the GCIO Office) as well as the CISO fit within the Organisations. Because of the way in which all IT functions and capabilities (including IT staff) for the public healthcare sector are centralised in IHiS, it is not readily apparent whether SingHealth or IHiS is responsible for the actions of the GCIO and CISO.

46 As mentioned at paragraph 9 above, every Cluster has a GCIO and CISO. It is not disputed that the SingHealth GCIO and SingHealth GCIO Office are operationally part of SingHealth and its organisational structure. The SingHealth GCIO is positioned at the top of and is in charge of the SingHealth GCIO Office, through which he carries out services and owes responsibilities to SingHealth in terms of overseeing SingHealth's IT systems. In SingHealth, the SingHealth GCIO and his office have a number of duties. These include:

(a) the SingHealth GCIO is responsible for updating the SingHealth Board of Directors on important IT security matters and attends the SingHealth Board IT Committee ("**ITC**") meetings. For example, the SingHealth GCIO provides SingHealth's Risk Oversight Committee ("**ROC**") with information relating to proposed or implemented measures to improve SingHealth's IT security, such as encryption of data in SingHealth's servers, monitoring of unusual access to the EMR and outgoing network traffic, and phishing exercises conducted on SingHealth staff. The SingHealth GCIO also informs the ROC about major IT security incidents in SingHealth's network, remediation of cybersecurity weaknesses observed in SingHealth's servers, and the status of SingHealth's compliance with IT security standards, such as the IT-SPS;

(b) the SingHealth GCIO sits on several SingHealth management level committees that have oversight over IT matters in SingHealth, specifically the Cluster IT Council ("**CITC**"), Electronic Medical Record Steering Committee ("**EMRSC**") and Enterprise Resource Planning Steering Committee ("**ERPSC**").[8] The SingHealth GCIO Office is also the secretariat of the CITC, the overall governing body for IT matters across the SingHealth Cluster;

(c) the SingHealth GCIO Office oversees SingHealth's IT operations and security and exercises oversight over the IHiS Delivery Group's administration and implementation of policies;

(d) the SingHealth GCIO Office prepares and presents for approval, papers on IT security proposals and budgets, including various annual IT work plans and budgets to SingHealth's management, management committees and board committees, such as the CITC and ITC. The SingHealth GCIO works with the respective SingHealth PHIs to prepare the IT workplan[9] for each SingHealth PHI;

(e) the SingHealth GCIO Office tracks the implementation of audit remediation measures recommended by MOHH's Group Internal Audit division ("**GIA**") [10] according to the timeline agreed between IHiS and GIA;[11] and

(f) the SingHealth GCIO and GCIO Office also play a key role in SingHealth's staff IT security education and awareness initiatives by developing various security policies pertaining to cybersecurity in accordance with the IT-SPS, such as the SingHealth IT Acceptable Use Policy, the SingHealth Response Plan for Cyber Attacks (Version 3.0) ("**SingHealth RP CA**"), the standard operating procedure ("**SOP**") for Incident Communication and Escalation and the SingHealth Data Access Policy. The SingHealth GCIO also sends out memos to all SingHealth staff in relation to IT security risks and staff training initiatives, e.g. phishing exercises.

[8] See paragraph 66 below for more details on the CITC and other board committees in SingHealth with oversight over IT matters.
[9] An IT workplan would typically include IHiS' direction for implementation of IT initiatives, including IT security initiatives (such as Advanced Threat Protection and hard disk encryption) for the financial year.
[10] The scope of the GIA's audits are discussed at paragraphs 71 to 73 below.
[11] The SingHealth GCIO Office does not verify whether the audit remediation measures have been implemented. The GIA would validate if the remediation measures had in fact been performed and update SingHealth management accordingly.

47 Similarly, as mentioned at paragraph 9 above, it is not disputed that the SingHealth CISO is charged with security oversight for SingHealth and reports to the SingHealth GCIO directly on security matters. The SingHealth CISO does not have any staff reporting under him and relies on the IHiS Delivery Group (specifically the SMD) for their technical expertise on security and operational matters. The SingHealth CISO has a key role in the organisational structure of SingHealth with regard to IT security. Under the IT security incident reporting processes developed and/or adopted by SingHealth, the SingHealth CISO has substantial responsibilities including the assessing, monitoring, and coordinating of responses to such incidents. He is accountable for the actions of incident response functions and is responsible for making regular, direct reports to the SingHealth GCIO, SingHealth management and other relevant parties such as the CSG.

48 On balance, while IHiS employees deployed to fill the SingHealth GCIO or CISO role may owe concurrent duties and responsibilities to IHiS, to the extent that they are carrying out the functions of the SingHealth GCIO or CISO, it is not disputed that they act on behalf of SingHealth. Insofar as they perform the work and operate on behalf of SingHealth, the Commissioner finds that the actions of the SingHealth GCIO and CISO as well as the SingHealth GCIO Office should be attributed to SingHealth.

(b) Whether the Organisations complied with their obligations under section 24 of the PDPA

49 Section 24 of the PDPA requires an organisation to protect the personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks (the "**Protection Obligation**").

50 Pursuant to section 11(1) of the PDPA, the reasonableness of the security arrangements made is to be objectively determined, having regard to what a reasonable person would consider appropriate in the circumstances. The following factors as set out in the Advisory Guidelines on Key Concepts in the PDPA (revised 27 July 2017) (at [17.2]) are taken into consideration in assessing the reasonableness of security arrangements:

(a) the nature of the personal data;

(b) the form in which the personal data has been collected (e.g. physical or electronic); and

(c) the possible impact to the individual concerned if an unauthorised person obtained, modified or disposed of the personal data.

51 In assessing the reasonableness of the security arrangements adopted by the Organisations, the Commissioner took into consideration the fact that medical data is personal data of a sensitive nature which should be accorded a higher standard of protection.[12] The health sector handles some of the most sensitive personal data and patients have the right to expect that the data will be looked after.[13]

52 As observed in *Re The Cellar Door Pte Ltd and Global Interactive Works Pte Ltd* [2016] SGPDPC 22, "reasonable security arrangements" for IT systems must be sufficiently robust and comprehensive to guard against a possible intrusion or attack:[14]

> "**Another important aspect of a "reasonable security arrangement" for IT systems is that it must be sufficiently robust and comprehensive to guard against a possible intrusion or attack**. For example, it is not enough for an IT system to have strong firewalls if there is a weak administrative password which an intruder can "guess" to enter the system. The nature of such systems require there to be sufficient coverage and an adequate level of protection of the security measures that are put in place, since a single point of entry is all an intruder needs to gain access to the personal data held on a system. **In other words, an organisation needs to have an "all-round" security of its system. This is not to say that the security measures or the coverage need to be "perfect", but only requires that such arrangements be "reasonable" in the circumstances.**"
>
> [Emphasis added.]

53 The public healthcare sector is heavily reliant on IT and a wide variety of IT systems that hold personal data are employed as part of a healthcare institution's operations.[15] In particular, the SCM system is hosted in H-Cloud and the SCM database contains the full medical records of all SingHealth's patients, which is very sensitive personal information. It is

[12] *Re Aviva Ltd* [2018] SGPDPC 4 at [17].
[13] UK, ICO, Health Sector Resources <https://ico.org.uk/for-organisations/resources-and-support/health-sector-resources/>.
[14] *Re The Cellar Door Pte Ltd* at [29].
[15] These include clinical systems that provide direct patient care to administrative and infrastructure systems that automate processes and workflow and facilitate sharing of information and communications across teams within and outside of the institution.

therefore critical to protect the security and confidentiality of such medical records. As highlighted in the Advisory Guidelines for the Healthcare Sector (updated 28 March 2017) (at [4.2]):

> "In relation to the Protection Obligation, the PDPA requires an organisation to make reasonable security arrangements to protect personal data in its possession or under its control. There is no 'one size fits all' solution for organisations to comply with the Protection Obligation. **Generally, where the personal data stored is regarded as more confidential and where the adverse impact to individuals is significantly greater if such personal data were inadvertently accessed (e.g. relating to sensitive medical conditions), tighter security arrangements should be employed. Healthcare institutions should consider the nature of the personal data in their possession or under their control (as the case may be) to determine the security arrangements that are reasonable and appropriate in the circumstances**."
>
> [Emphasis added.]

Whether SingHealth complied with its Protection Obligation

54 As an organisation subject to the data protection provisions under the PDPA, SingHealth has the primary responsibility of ensuring that there are reasonable security arrangements in place to protect the personal data in its possession or under its control,[16] regardless of whether SingHealth has appointed a data intermediary to process patient personal data on its behalf.

55 While SingHealth may outsource the activities necessary to protect the personal data in the SCM database by engaging IHiS to maintain and secure its IT network and the SCM database, SingHealth has a duty to ensure that any data intermediary that processes personal data on its behalf complies with the PDPA.[17] This means that SingHealth can still be liable for a data breach for failing to meet its responsibility, even though IHiS was found to have its own responsibility, and *vice versa*.[18]

56 The Commissioner takes this opportunity to reiterate that while organisations may outsource work to vendors, the responsibility for complying with statutory obligations under the PDPA may not be delegated:[19]

---

[16] Clause 5.1.1 of the DPP expressly states that Clients (i.e. SingHealth) will at all times remain in control over Client Data (i.e. the personal data of SingHealth's patients).
[17] See *Re Smiling Orchid (S) Pte Ltd and others* [2016] SGPDPC 19 at [46].
[18] *Re Social Metric Pte Ltd* at [16], citing *Re Smiling Orchid*. See also *Re Singapore Telecommunications Limited and another* [2017] SGPDPC 4 and *Re Aviva Ltd and another* [2016] SGPDPC 15.
[19] *Re WTS Automotive Services* [2018] SGPDPC 26 at [23].

> "Further, organisations should take note that while they may delegate work to vendors to comply with the PDPA, **the organisations' responsibility for complying with statutory obligations under the PDPA may not be delegated**."
>
> [Emphasis added.]

57 Having said that, our earlier decisions have recognised that there may be different responsibilities that an organisation or data intermediary may undertake under the PDPA. In *Re Social Metric Pte Ltd* [2017] SGPDPC 17, the Commissioner explained that where the data processing activities are carried out by the organisation's external vendor, the organisation has a *supervisory or general role for the protection of the personal data*, while the data intermediary has a more direct and specific role in the protection of personal data arising from its direct possession of or control over the personal data.[20]

58 In this case, on the basis of the Organisations' representations and evidence in these proceedings, the Commissioner is satisfied that SingHealth had some security arrangements in place to meet its supervisory role for the protection of the personal data, such as by maintaining oversight and control over IHiS' processing of the SCM database. However, the SingHealth CISO's failure to comply with the IT security incident reporting processes and failure to exercise independent judgement call into question whether SingHealth had taken reasonable and appropriate measures to protect the personal data in the SCM database from unauthorised access and copying. More importantly, it points to a larger systemic issue within the organisation.

59 To begin with, parties should put in place a contract that sets out the obligations and responsibilities of a data intermediary to protect the organisation's personal data and the parties' respective roles, obligations and responsibilities to protect the personal data.[21] The foreign data protection authorities have taken the position that a data controller that outsources the processing of its personal data to data processors must take all reasonable steps to protect that information from unauthorised use and disclosure while it is in the hands of the third-party processor.

---

[20] *Re Social Metric Pte Ltd* at [16], citing *Re Smiling Orchid*.
[21] *Re Singapore Telecommunications Limited* at [14].

60 According to the Information Leaflet on the Outsourcing the Processing of Personal Data to Data Processors published by the Hong Kong Office of the Privacy Commissioner for Personal Data's ("**PCPD**"),[22] the primary means by which a data user may protect personal data entrusted to its data processor is through a contract.[23] The PCPD recommends that the following obligations should be imposed on data processors:

> "**How to comply with the requirements**
>
> *Through contractual means*
>
> **The primary means by which a data user may protect personal data entrusted to its data processor is through a contract**. In practice, data users often enter into contracts with their data processors for the purpose of defining the respective rights and obligations of the parties to the service contract. To fulfil the new obligations under DPP2(3) and DPP4(2), data users may incorporate additional contractual clauses in the service contract or enter into a separate contract with the data processors.
>
> The types of obligations to be imposed on data processors by contract may include the following:-
>
> (a) **security measures required to be taken by the data processor to protect the personal data entrusted to it and obligating the data processor to protect the personal data by complying with the data protection principles** (The security measures that are appropriate and necessary for a data user will depend on the circumstances. Basically, the data processor should be required to take the same security measures the data user would have to take if the data user was processing the data himself);
>
> (b) timely return, destruction or deletion of the personal data when it is no longer required for the purpose for which it is entrusted by the data user to the data processor (it is for the parties to agree the appropriate number of days);
>
> (c) **prohibition against any use or disclosure of the personal data by the data processor for a purpose other than the purpose for which the personal data is entrusted to it by the data user**;
>
> (d) absolute prohibition or qualified prohibition (e.g. unless with the consent of the data users) on the data processor against sub-contracting the service that it is engaged to provide;
>
> (e) where sub-contracting is allowed by the data user, the data processor's agreement with the sub-contractor should impose the same obligations

[22] Hong Kong, PCPD, Outsourcing the Processing of Personal Data to Data Processors (September 2012) <https://www.pcpd.org.hk/english/publications/files/dataprocessors_e.pdf>. Under Hong Kong law, a data user is to take all reasonably practicable steps to safeguard the security of personal data held by it. Where personal data is entrusted to a data processor, a data user is responsible for any act done by the data processor.

[23] However, the PCPD also recognised that other means of compliance, such as being satisfied that data processors have robust policies and procedures in place and having the right to audit and inspect, may be used.

in relation to processing on the sub-contractor as are imposed on the data processor by the data user; where the sub-contractor fails to fulfil its obligations, the data processor shall remain fully liable to the data user for the fulfilment of its obligations;

(f) **immediate reporting of any sign of abnormalities** (e.g. audit trail shows unusual frequent access of the personal data entrusted to the data processor by a staff member at odd hours) **or security breaches by the data processor**;

(g) **measures required to be taken by the data processor (such as having data protection policies and procedures in place and providing adequate training to its relevant staff) to ensure that its relevant staff will carry out the security measures and comply with the obligations under the contract regarding the handling of personal data**;

(h) **data user's right to audit and inspect how the data processor handles and stores personal data**; and

(i) consequences for violation of the contract.

The above list is not exhaustive and data users may need to make adjustments or to include additional obligations on data processors under the contract having regard to factors such as the amount of personal data involved, the sensitivity of the personal data, the nature of the data processing service and the harm that may result from a security breach."

[Emphasis added.]

61 In a similar vein, the Office of the Privacy Commissioner of Canada's ("**OPC**") guidance note, Privacy and Outsourcing for Businesses,[24] states that organisations that outsource the processing of personal information must be satisfied that the third party has policies and processes in place, including training for its staff and effective security measures, to ensure that the information in its care is properly safeguarded at all times:

"The *Personal Information Protection and Electronic Documents Act* (PIPEDA) — Canada's federal private-sector privacy law – **requires organizations to take privacy consideration into account when considering outsourcing to another organization**.

There is nothing in PIPEDA that prevents organizations from outsourcing the processing of data.

However, regardless of where information is being processed—whether in Canada or in a foreign country—organizations subject to PIPEDA must take all reasonable steps to protect that information from unauthorized uses and disclosures while it is in the hands of the third-party processor.

[24] Canada OPC, Privacy Topics – Privacy and Outsourcing for Businesses (January 2014) <https://www.priv.gc.ca/en/privacy-topics/outsourcing/02_05_d_57_os_01/>.

> **Organizations must also be satisfied that the third party has policies and processes in place, including training for its staff and effective security measures, to ensure that the information in its care is properly safeguarded at all times**."
>
> [Emphasis added.]

62 The position taken by the foreign data protection authorities is consistent with the Commissioner's views in *Re Smiling Orchid*. There should be a clear meeting of minds as to the services the service provider has agreed to undertake and organisations must *follow through with procedures* to check that the outsourced provider is delivering the services:[25]

> "Data controllers that engaged outsourced service providers have to be clear about the nature and extent of services that the service provider is to provide. **There must be a clear meeting of minds as to the services that the service provider has agreed to undertake, and this should be properly documented**. **Data controllers should follow through with the procedures to check that the outsourced provider is indeed delivering the services.** In the absence of such clarity of intent and procedures, it is risky to hold that the outsourced service provider is a data intermediary."
>
> [Emphasis added.]

63 Having reviewed the policy documents at paragraph 42 above, the Commissioner finds that IHiS' duties and obligations as a data intermediary are clearly set out and properly documented in the policy documents. In particular:

(a) the IT-SPS sets out IHiS' roles and responsibilities, including to design procedures and processes needed to implement the IT security policies and standards as described in the IT-SPS;[26] and

(b) the DPP provides guarantees of security of the personal data processed on behalf of SingHealth as it expressly states that IHiS shall exercise reasonable care in protecting SingHealth's personal data and shall ensure that it implements and maintains appropriate security measures when processing personal data on behalf of SingHealth.[27]

---

[25] *Re Smiling Orchid* at [51]. See also *Re Singapore Cricket Association & Ors*. [2018] SGPDPC 19, where the Commission reiterated that organisations that engage service providers to process personal data on their behalf should clarify and properly document the nature and extent of service provided.
[26] Clause 6.1.1 of the IT-SPS.
[27] Clause 1.1.3 of the DPP:

> "As IT professionals who support healthcare organisations, IHIS acts as a "data intermediary" in relation to Client Data, **will exercise reasonable care in protecting Client Data from unauthorised access,**

64 The above policy documents evidence the parties' intentions to be contractually bound by, and define the scope of the duties and obligations set out therein.

65 Additionally, SingHealth has developed and implemented a number of data protection policies and practices, which were communicated to its staff. These include:

(a) a Data Protection Policy, which explains how SingHealth institutions handle personal data and is available to the public on SingHealth's website and at its premises;

(b) a PDPA Employee Standards Manual, which is a resource and guide for SingHealth employees regarding SingHealth's obligations under the PDPA;

(c) a dedicated intranet page for PDPA training materials, which is accessible to all staff;

(d) a Master Data Share Agreement that SingHealth entered into with its subsidiary institutions to regulate the sharing of information among the SingHealth institutions;

(e) a Data Access Approval Policy, which sets out the policy and procedure for handling data access requests from data subjects at the SingHealth level; and

---

> **collection, use, disclosure, copying, modification, disposal or similar risks** (our "**Protection Obligation**"), and we undertake steps to ensure that we do not retain personal data longer than is required for business or legal purposes (our "**Retention Obligation**")."
>
> [Emphasis added.]

Clause 11.1.1 of the DPP:

> "The principles under which we discharge our Protection Obligations as data intermediary under the PDPA for Client Data are as follows:
>
> 11.1.1 When Handling Client Data on behalf of Clients in connection with such services as IHiS may provide to Clients from time to time at Clients' request, **IHiS shall ensure that it implements and maintains appropriate security measures to ensure the security of the Client Data**.
>
> 11.1.2 In doing so, IHiS may be required to appoint vendors to advise on and execute the appropriate data protection measures, and Clients authorise IHiS to appoint such vendors as may be necessary to perform tasks in connection with meeting its obligations under Section 25 *[sic.]* PDPA under its engagement with the Clients."
>
> [Emphasis added.]

(f) a Data Breach Management Policy, which sets out the policy and procedure for the implementation of SingHealth's personal data breach management programme to manage personal data breaches effectively.[28]

SingHealth management and board oversight of IT operations and security

66 Apart from the policy documents, there is evidence that SingHealth maintained oversight of IT operations and security through various oversight and auditing mechanisms, such as through the following board and management committees:

(a) SingHealth's senior management and Board members are apprised of IT matters, such as IT audits and assessments, and the budgeting of IT projects, by the SingHealth GCIO Office;

(b) other than the SingHealth Board of Directors, there are three Board committees that have oversight of IT security matters and meet regularly throughout the year:

(i) the ITC: a Board committee comprising Board members and co-opted members from external institutions who have IT expertise. Senior management representatives from SingHealth such as the Group CEO ("**GCEO**") and Deputy Group CEO, as well as the SingHealth GCIO attends the ITC meetings. ITC approves the various annual IT workplans for the SingHealth Cluster, which are prepared by the SingHealth GCIO and the IHiS Delivery Group; and

(ii) the Audit Committee ("**AC**") and the ROC: where audits and key risks relating to cyber security matters, such as SingHealth's compliance with and key cyber security initiatives undertaken as part of the IT-SPS, and efforts to raise IT user security awareness, are deliberated upon. The ROC receives updates from the SingHealth GCIO on proposed or implemented measures to improve SingHealth's IT security;[29]

[28] In the present case, as the suspicious circumstances were first observed by IHiS staff from the IHiS Systems Management Department, the cyber security incident reporting framework which was followed was IHiS' IR-SOP.

[29] These include updates on the encryption of data in SingHealth's servers, monitoring of unusual access to the EMR and outgoing network traffic, and phishing exercises conducted on SingHealth staff.

(c) at the management level, the CITC is the overall governing body for IT matters across the SingHealth Cluster. The CITC reports to the ITC.[30] The CITC meets monthly to review and endorse SingHealth's Cluster-wide IT projects and initiatives and to oversee and review the IT security program. Its role is to ensure that IT strategy and investments are aligned with the business strategy and IT architecture of the Cluster, resulting in the effective and efficient use of IT in enabling SingHealth to achieve its goals. The SingHealth GCIO sits on the CITC. There are two further sub-committees under the CITC:

(i) the ERPSC; and

(ii) the EMRSC, which is the central governance body to oversee EMR access audit and continuous access monitoring requirements. The EMRSC members comprise of the SingHealth GCIO as well as the Directors of Medical Informatics of the various PHIs in SingHealth.

Operational measures

67 In addition to the board and management level oversight, the Commissioner finds that through the SingHealth GCIO and GCIO Office, SingHealth also followed through with operational procedures and checks to ensure that IHiS carried out its functions to protect their personal data.

68 The SingHealth GCIO Office exercises oversight of the IHiS Delivery Group's administration of policies. It monitors and verifies that policies are carried out and issues of security are addressed primarily through various operational meetings between the SingHealth GCIO Office and the IHiS Delivery Group, such as:

(a) the monthly SingHealth IT Management, Communication and Coordination Meeting chaired by the SingHealth GCIO, where issues of cyber security are discussed, allowing the SingHealth GCIO to track and ensure follow up of any outstanding remediation measures to be done;

[30] SingHealth's GCEO chairs the CITC, and DGCEO (OT&I) is the Deputy Chair. The CITC members include the other SingHealth DGCEOs and the heads of the various PHIs in SingHealth. The SingHealth GCIO Office is the secretariat of the CITC.

(b) regular meetings between the SingHealth GCIO Office Application Directors and the individual IHiS Delivery Group teams (e.g. the SMD), which further allows for cyber security issues and policy compliance to be tracked; and

(c) *ad hoc* meetings between the SingHealth GCIO Office and the relevant IHiS Delivery Group teams to track and ensure that detected vulnerabilities in the SingHealth network are addressed.

69 As mentioned at paragraph 72 below, the SingHealth CISO also keeps track of the timelines agreed between IHiS and the GIA on the audit remediation measures. In the circumstances, the Commissioner finds that there are governance and audit mechanisms in place for SingHealth to maintain oversight and control over IHiS' processing of the SCM database.

Audits and risk management

70 The security measures put in place by IHiS are also subject to regular audits. The SingHealth CISO conducts yearly Critical Information Infrastructure ("**CII**") risk assessments on SingHealth's mission-critical IT systems (i.e. SingHealth's SCM system) on behalf of SingHealth. This exercise is overseen by the SingHealth GCIO and the SingHealth CISO relies on technical input from members of the IHiS Delivery Group in assessing the risks or threats to the CII, the controls in place and the steps that should be taken to improve on the existing controls. The SingHealth CISO's assessment is presented to the SingHealth ITC.

71 Separately, MOHH's GIA conducts a CSA CII Compliance Review on the SCM system annually to ascertain if SingHealth, being a CII operator, has complied with CSA's requirements for the CII.

72 The GIA also conducts an annual audit of SingHealth's IT systems.[31] The GIA identifies and prioritises the key risk areas (including for cyber security) and comes up with the annual audit plan together with input from SingHealth management for the SingHealth

[31] The GIA is an independent centralised internal audit division housed within MOHH which audits the Clusters and IHiS. Audit findings from the GIA are presented directly to the AC and the ROC. Their findings are also addressed by the IHiS Board Audit and Risk Committee. The GIA reports to the MOHH Board Audit and Risk Committee, which comprises all the Audit Committee Chairmen from all the MOHH subsidiaries (including SingHealth and IHiS).

AC's review and approval. The SingHealth CISO coordinates GIA audits by being the parties' point of contact and keeps track of the timeline agreed between IHiS and the GIA on the audit remediation measures.

73 By way of example, in FY 2016, the GIA planned an audit on IHiS' H-Cloud data centre and engaged external providers to perform an IT security penetration test from three PHI systems, one of which was from SGH to H-Cloud (the "**H-Cloud Pen-Test**"). The plan for the H-Cloud Pen-Test was presented to and approved by the SingHealth AC on 16 May 2016 and the H-Cloud Pen-Test was conducted in early January 2017.

74 As the H-Cloud Pen-Test was an audit of IHiS' H-Cloud, the finalised audit report (the "**GIA Audit Report**") was addressed to the CEO of IHiS. However, the audit findings (including the security risks) and the follow up actions and measures to be taken by IHiS were brought to the attention of SingHealth's senior management and were discussed at various board committees and management committees within SingHealth.

75 Between May 2017 and October 2017, the GIA (which was tasked with eventually validating that remediation measures had been carried out) presented the results and observations from the H-Cloud Pen-Test to the SingHealth Board AC, ROC and ITC and provided updates on the remediation measures and implementation timelines being undertaken by IHiS to rectify the weakness identified in the GIA Audit Report. This shows that SingHealth's various board committees were kept abreast of the follow up for the remediation measures by the GIA.

76 One area that had previously been identified as a potential issue in the operational monitoring of the remediation of the audit findings was in respect of the implementation by IHiS of firewall rules on the SGH Citrix Servers to block remote desktop protocol traffic from end-user workstations. In its further representations, SingHealth provided evidence that the SingHealth GCIO Office, through the SingHealth CISO, had been tracking the status of the remediation of these outstanding issues. The IHiS Delivery Group had informed the SingHealth CISO on more than one occasion that the implementation of the software firewall rules as a remediation measure had been completed by 7 August 2017. As the implementation of the software firewall rules are a matter of configuration of the existing SGH Citrix Servers without the need for procurement of additional equipment, it is not unreasonable for the SingHealth

CISO to have relied on IHiS Delivery Group to provide him with an update after implementation. In retrospect, the SingHealth CISO could have asked for evidence (e.g. screenshots) demonstrating that the software firewall had been turned on and was effective in blocking remote desktop protocol traffic from end-user workstations. But this would have been a level of operational verification that the SingHealth CISO can reasonably expect the IHiS Delivery Group to have done before they reported up to him that this audit finding had been remediated. Having considered SingHealth's further representations, and the evidence provided, the Commissioner accepts that SingHealth had exercised reasonable oversight in respect of the implementation of the software firewall rules.

77 A similar position was taken by the OPC in the Canadian Personal Information Protection and Electronic Documents Act ("**PIPEDA**") Case Summary #2007-365,[32] which relates to the disclosures by the Society for Worldwide Interbank Financial Telecommunication ("**SWIFT**") of personal information to US authorities. The OPC reviewed the contract in place between SWIFT and the banks, as well as the other means available to the banks to ensure that SWIFT is providing a comparable level of protection. It found that the banks had fulfilled their obligations under Principle 4.1.3 of the PIPEDA, citing the various oversight and auditing mechanism, such as the development and implementation of a highly sophisticated and elaborate set of security measures, the cooperative oversight and technical oversight group:

> "SWIFT and its members have **collaboratively developed and implemented a highly sophisticated and elaborate set of security measures to ensure the integrity, confidentiality, security and reliability** of the financial messages that SWIFT delivers.
>
> **SWIFT reports back to its committees and boards through its Annual Report and through the security audit report** (it should be noted that these reports encompass far more than personal information handling practices).
>
> Although some of the contractual language appears to place SWIFT in control of how its system is used and, by extension, how personal information in its possession is handled, it is nevertheless also obliged to maintain confidentiality of information.
>
> Furthermore, the Assistant Commissioner noted that there are other means by which the banks, as members and users of the SWIFT system, can ensure that a comparable level of protection is in place, particularly with respect to **the cooperative oversight and technical oversight groups. Through these various oversight and auditing mechanisms, and through the contractual**

[32] OPC, PIPEDA Case Summary #2007-365, Responsibility of Canadian financial institutions in SWIFT's disclosure of personal information to US authorities considered (2 April 2007) <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2007/pipeda-2007-365/>.

language and various security measures in place, she was satisfied that the banks are meeting their obligations under Principle 4.1.3."

[Emphasis added.]

SingHealth CISO's failure to escalate incident

78 Notwithstanding, as described at paragraph 30 above, the Commissioner observes that the SingHealth CISO failed to comply with the various incident response policies and SOPs. The SingHealth CISO's role in relation to cyber incidents are detailed in the following IT security incident reporting policy documents:

(a) under the SingHealth RP CA, the SingHealth CISO's role is to:

(i) develop and align IT security incident handling and response policies and processes;

(ii) under the Security Incident Response Plans for various scenarios, e.g. Malware Infection and Data Loss/Leakage, upon being alerted, the SingHealth CISO is responsible for crucial steps, including:

(A) to review and classify the incident and notify the relevant personnel, such as the SingHealth GCIO, SingHealth's Corporate Communication Department, the CSG, and the management of affected SingHealth institutions ("**Relevant Personnel**") within 30 minutes of receiving the alert;

(B) to prepare the incident report and provide periodic containment and incident closure updates to the Relevant Personnel; and

(C) for the post mortem, to finalise and submit the incident report to the Relevant Personnel, and update the SOP for such incidents.

(b) under the IR-SOP, the SingHealth CISO likewise has a direct line of reporting to the SingHealth GCIO and the following responsibilities in a security incident:

(i) accountable for the actions of the incident response team and incident response functions;

(ii) responsible for making regular, direct reports to the SingHealth GCIO, the CSG and the management of SingHealth institutions;

(iii) perform post-incident review of the incident to improve processes;

(iv) coordinate with SingHealth's Corporate Communication Department;

(v) where applicable, report to law enforcement authorities; and

(vi) endorse IT security incident handling and response processes.

79 As mentioned at paragraph 47 above, the SingHealth CISO has a key role in the organisational structure of SingHealth with regards to IT security, alongside the SingHealth GCIO. Under the IT security incident reporting processes developed and/or adopted by SingHealth, the SingHealth CISO has substantial responsibilities including assessing, monitoring, and coordinating responses to such incidents. He is accountable for the actions of the incident response functions and is responsible for making regular, direct reports to the SingHealth GCIO, SingHealth management and other relevant parties such as the CSG.

80 Cyber security incidents are investigated by the IHiS SIRT, which is led by the SIRM. As the SingHealth CISO does not have any staff reporting under him, the SingHealth CISO relies on the IHiS Delivery Group for their technical expertise on security and operational matters. Under the IR-SOP, the SIRM is responsible for leading the effort of the SIRT and coordinating input from the SIRT members. The SIRM reports to the SingHealth CISO. In turn, the SingHealth CISO is accountable for the actions of the SIRT and is responsible for escalating any issues to the SingHealth GCIO Office.

81 In this case, even though the SingHealth CISO was informed of suspicious activities showing multiple failed attempts to log in to the SCM database using invalid credentials, or accounts that had insufficient privileges in mid-June 2018, and the attack and remediation efforts on 4 July 2018, the SingHealth CISO did not escalate these security events. Rather, he wholly deferred to the SIRM's assessment as to whether an incident was reportable (who operated erroneously under the misapprehension that a cyber security incident should only be escalated when it is "confirmed") when he should have exercised independent judgement to escalate the incident to the SingHealth GCIO. To his mind, at the time that he was informed of these suspicious activities, they were only potential breaches and were not confirmed security incidents as investigations were still underway. This does not comply with the IR-SOP. Besides

failing to exercise his independent judgement, it would appear that the SingHealth CISO also failed to understand the significance of the information provided to him or to grasp the gravity of the events that were happening.

82 In this respect, the findings of the COI are relevant. Having thoroughly examined the incident response up to 10 July 2018, including the sequence of events and the state of mind of the persons involved, the COI found that with regard to the incidents on 4 July 2018, the SingHealth CISO's response was "clearly lacking, and displayed an alarming lack of concern".[33] It was clear at that point that a CII system had potentially been breached. The SingHealth CISO should have recognised it as a Category 1 reportable security incident and taken steps to escalate the matter immediately but he did not do so. Instead, he "effectively abdicated to [the SIRM] the responsibility of deciding whether to escalate the incident".[34]

83 Furthermore, although the SingHealth CISO was accountable for the actions of the SIRT under the IR-SOP, the COI found that the SingHealth CISO did not provide any significant degree of leadership in sharing information, coordinating investigations and remediation efforts across the various IHiS teams. Instead, the SingHealth CISO "did nothing, and simply left [the SIRM] and the rest of the SIRT to their own devices in the investigation of the matter and remediation efforts".[35]

84 In the circumstances, the Commissioner finds that the SingHealth CISO failed to discharge his duties. For the reasons set out at paragraphs 47 to 48 above, the SingHealth CISO's failure to comply with the incident reporting SOPs is a lapse that is attributable to SingHealth. While the attacker had already gained access to the SCM network and SCM database by that time, given the substantial volume of sensitive medical personal data held in the SCM database, it is reasonable to expect that someone in the SingHealth CISO's position, with the experience and stipulated responsibilities under the IT security incident reporting processes, should have been more familiar with the incident reporting standards, showed greater initiative and exercised independent judgement to escalate the incident to the SingHealth GCIO. However, the SingHealth CISO's conduct in this case fell far short of what a reasonable person would expect from someone in his position.

[33] Public COI Report at [514].
[34] Public COI Report at [514].
[35] Public COI Report at [514].

85 In its representations, SingHealth referred to evidence of communications between the SingHealth CISO and SIRT personnel between 13 June 2018 and 9 July 2018, which showed that the SingHealth CISO raised queries and sought updates while the SIRT was conducting investigations into the cyber security incident. Having reviewed the evidence submitted by SingHealth, the Commissioner finds that the SingHealth CISO had not acted reasonably and failed to discharge his responsibilities. Apart from raising a few questions with regard to the suspicious activities when they first surfaced on 13 June 2018, the SingHealth CISO failed to provide any input or guidance to the team or query whether the matter should be escalated. Rather, the evidence showed that security incidents were handled without sufficient regard for the importance of protecting personal data and discharging its responsibilities properly.

86 SingHealth's representations also drew attention to an important point about the role of the SingHealth CISO from an organisational structure perspective. Because all IT functions and capabilities for the public healthcare sector, including the domain expertise and technical capabilities required to investigate and respond to IT security incidents, are centralised in IHiS, in effect, the SingHealth CISO and GCIO Office have little choice but to rely on the IHiS SMD for their oversight on cybersecurity incidents.

87 The SingHealth GCIO is supported by the GCIO Office, which has a staff strength of about 50 IHiS employees. Together, they are collectively responsible for 11 institutions, with an estimated 30,000 employees, 400-odd IT systems and 350 to 500 IT projects. The SingHealth CISO's responsibilities in the GCIO Office are also relatively broad and include:

(a) working on IT risk assessments;[36]

(b) liaising with the GIA and IHiS Delivery Group for audit confirmation, coordinating progress updates and following-up on any audit findings or observations;

(c) being part of the security incident response and reporting process;[37] and

[36] The SingHealth CISO covers at least 4 risk assessments (enterprise risks, CII risks etc) each year from the IT perspective. Each assessment would stretch over a few months depending on the complexity of the matter. The SingHealth CISO would also follow up with the IHiS Delivery Group to check on the remediation / implementation status.

[37] The SingHealth CISO would liaise with the IHiS SMD for security event escalation about 3 to 4 times a month. In such instances, other IHiS Delivery Group colleagues would inform the SingHealth CISO about potential security issues. The SingHealth CISO would liaise with the SMD for follow up and remediation, and to also obtain confirmation of remediation.

(d) assisting the SingHealth GCIO in raising end-user awareness of IT security in SingHealth.

88 Given the size and scale of SingHealth's IT systems and network and the large databases of sensitive medical personal data that SingHealth is responsible for, it is reasonable to expect that considerable resources would have been devoted to the SingHealth CISO to carry out operational and security oversight of SingHealth's IT systems. However, the SingHealth CISO (who is the only staff who has a portfolio specific to security) worked alone and had no staff reporting under him. As a result of this arrangement, when the SingHealth CISO was on medical leave between 20 June 2018 and 3 July 2018, there was no one other than the IHiS SIRM to cover the SingHealth CISO's duties and provide guidance on the investigation.

89 The SingHealth CISO's failure to discharge his duties is also not a one-off incident that would have been difficult to foresee.[38] Rather, it revealed a systemic problem in the way the SingHealth GCIO Office, specifically the SingHealth CISO function, is staffed. The SingHealth CISO did not have the resources or the technical and IT security expertise for him to properly fulfil his functions. For example, he should have had a team within SingHealth to support him and provide adequate cover when he is away. It was evident from the SingHealth CISO's response to the Data Breach that the existing arrangements are inadequate. As this organisational arrangement failed to meet the reasonable standards expected of an organisation of SingHealth's size, the Commissioner finds that SingHealth had failed to put in place reasonable security arrangements to protect the personal data in its possession or under its control from unauthorised access and copying.

90 In this regard, SingHealth made representations submitting that it relies on and requires IHiS to ensure that the staff they deploy to carry out functions provided by IHiS, such as the SingHealth GCIO and CISO, are appropriately qualified and trained to discharge their duties and do so responsibly. SingHealth has no control over the organisational structure, how the CISO and SIRT is set up, or how the SingHealth CISO has to rely on the investigation findings and updates of the SIRT and other teams before making a report upwards or over manpower allocation. It also emphasised that SingHealth shares an atypical relationship with IHiS which goes beyond the typical relationship a vendor shares with a customer – IHiS is not an IT vendor but the MOH-designated IT arm of the public healthcare sector.

[38] See *Re BHG (Singapore) Pte Ltd* [2018] SGPDPC 16 at [25] – [28].

91 The Commissioner understands that this is the way the public healthcare sector is structured and is sympathetic to the fact that SingHealth may have had limited ability to influence the organisational structure. Nevertheless, insofar as SingHealth is an organisation as defined in section 2(1) of the PDPA and does not fall within any of the category of organisations that are excluded from data protection obligations under section 4(1) of the PDPA, SingHealth is required to demonstrate that it has complied with the obligations under the PDPA in the event of an investigation.[39]

92 In this regard, as emphasised in earlier decisions and at paragraph 54 above, it bears repeating that SingHealth has the *primary role and responsibility* of ensuring the overall protection of the personal data in its possession or under its control, even if it has engaged a data intermediary that has a duty to protect the personal data.[40] The fact that SingHealth is required to engage and rely on IHiS for all its IT services in accordance with MOH's policy does not absolve SingHealth from its responsibilities and obligations under the PDPA. Hence, these representations cannot absolve SingHealth from liability but the Commissioner recognises the exceptional set of circumstances in this case, and have taken them into consideration as mitigating factors in the directions that the Commissioner has made.

93 SingHealth also submitted that the errors of individuals within organisations should not in and of itself equate to a breach of section 24 of the PDPA unless the individual's errors points to a larger systemic issue within the organisation or an inadequacy of security arrangements which led to or caused the mistakes, lapses or poor judgement.

94 The Commissioner agrees that as a matter of principle, an error or flaw in the organisation's systems and processes does not automatically mean that the organisation failed to take reasonable security arrangements to protect personal data. As highlighted in *AIG Asia Pacific Insurance Pte Ltd* [2018] SGPDPC 8 (at [27] and [28]), the Commissioner will consider whether the organisation had implemented any security arrangements and if so, whether those arrangements are reasonable:

> "**The fact that personal data had been disclosed to an unauthorised party by an error or flaw in an organisation's systems and processes does not automatically mean that the organisation is liable under section 24 of the**

[39] Advisory Guidelines on Key Concepts in the PDPA at [6.3].
[40] See *Re The Management Corporation Strata Title Plan No. 3696 and Eagle Eye Security Management Services Pte Ltd* [2017] SGPDPC 11 at [16]; *Re The Cellar Door Pte Ltd* at [33] and [34].

> **PDPA** for failing to take reasonable security arrangements to protect personal data.
>
> For the purposes of section 24, the **Commissioner has to consider what security arrangements (if any) an organisation had implemented to prevent such unauthorised disclosure, and whether those arrangements are reasonable**."
>
> [Emphasis added.]

95 In the present case, as the Commissioner has found at paragraphs 87 to 89 above that the SingHealth CISO's failure to comply with the SOPs was emblematic of the inadequacy of the security arrangements, the Commissioner has already taken this into consideration before SingHealth submitted its representation.

96 Having carefully considered all the relevant facts and representations made by SingHealth, the Commissioner finds that while SingHealth had maintained oversight over IHiS' provision of IT operations and security through various levels of board, management and operational oversight and audit mechanisms, SingHealth had not taken sufficient security measures to protect the personal data in the SCM database from the unauthorised access and illegal copying. Accordingly, SingHealth has failed to meet its Protection Obligation and is in breach of section 24 of the PDPA.

Whether IHiS complied with its Protection Obligation

97 At the outset, as the personal data in the SCM database was in IHiS' possession, if not under its control, IHiS was obliged to implement reasonable security arrangements to protect the personal data in the SCM database.

98 It is accepted that the Data Breach was perpetrated by a skilled and sophisticated threat actor. The level of discipline and planning demonstrated during the Data Breach are characteristic of an APT actor, who used advanced methods that overcame enterprise security measures:

(a) the attacker took steps to conduct lateral movement and reconnaissance in order to avoid breaching the existing detection mechanisms IHiS had put in place, and could not have easily been noticed;

(b) the attacker used highly customised malware that evaded SingHealth's anti-virus software and security defences and could not have been detected by standard anti-malware solutions; and

(c) the attacker employed numerous customised and modified open-source scripts and tools that were manipulated to evade signature-based anti-virus detection.

99 Furthermore, the attacker deliberately and specifically targeted the SCM database and took active steps to ensure that it would remain undetected until it had reached the SCM database.

100 Hence, the key issue for determination is whether, despite the attacker's sophisticated and novel tactics, techniques and procedures, IHiS had done enough under section 24 of the PDPA to prevent the unauthorised disclosure.

IHiS' security arrangements at the material time

101 IHiS bases its security arrangements on the IT-SPS,[41] which is a policy based on international information security standards. The IT-SPS covers all the essential IT security domains, and prescribes the IT security policies, technical security standards and processes to be implemented by all public healthcare institutions, including policies on user access control and password management.

102 According to IHiS, it maintained a comprehensive IT security incident and response framework, which consists of three measures – prevention, detection and response, for all systems under its purview (including the SCM network during the time of the Data Breach). A brief summary of the measures taken for the SCM network is as follows:

(a) technical measures to prevent cyber security risks for:

(i) end-point security relating to SingHealth and IHiS issued end-point devices (e.g. workstations), such as the prohibition from use of personal devices on the SCM network, the use of anti-virus and anti-malware software;

[41] The current version of the IT-SPS was issued in 2014.

(ii) network security, such as creating network firewalls to segregate each network segment so as to ensure that only authorised network traffic is permitted to cross segments or zones;

(iii) H-Cloud security by implementing measures such as web application firewalls, physical separation of Virtual Data Centres, and Privileged Access Management;

(iv) database security, such as by running automated scripts which closely monitor the SCM database to detect and raise alerts for performance abnormalities, and keeping detailed access and audit logs which include information such as failed login attempts; and

(v) email security, such as anti-virus, anti-spam and attachment blocking technology;

(b) policies and processes to manage or otherwise deal with cyber security risks, which include:

(i) building awareness and educating staff on cyber security risks and IHiS' IT policies, such as by conducting IT security training, sending regular security alerts and conducting regular phishing exercises to create awareness and promote vigilance;

(ii) developing policies for users, such as the IT-SPS, the SingHealth Acceptable Use Policy, and the SingHealth End User Computing, Equipment and Network Policy and monitoring the compliance of users to these policies; and

(iii) conducting periodic reviews of the risks, controls and other measures of the security systems flagged by the GIA;

(c) detection measures to identify and pinpoint cyber security risks, such as continuous real-time monitoring and periodic testing; and

(d) risk assessment exercises carried out at various levels. For example, enterprise risk assessment and CII risk assessment exercises were conducted annually by the SingHealth CISO and overseen by the SingHealth GCIO.

103 At the material time, IHiS also had the following incident reporting processes and frameworks in place to ensure that cyber security incidents are appropriately escalated and addressed:

(a) the SIRF, which translates the requirements of the National Cyber Incident Response Framework[42] into the context of the PHIs; and

(b) the IR-SOP, which is IHiS' Cluster-level standard operating procedure for responding to security incidents.

104 Internally, IHiS also maintains a security incident classification framework identical to that used by CSA, and has developed internal reporting timelines for security incidents to be escalated to the CSG within IHiS.

105 Cyber security incidents are investigated by the IHiS SIRT. This team is led by the SIRM, and comprises of IHiS' Computer Emergency Response Team ("**CERT**") and lead personnel from IHiS Infrastructure Services and Application Services teams. It is the SIRM's responsibility to coordinate input from the SIRT members and to report to the SingHealth CISO. The SingHealth CISO's responsibility is to escalate any issues to the SingHealth GCIO.

106 As mentioned at paragraph 127 below, IHiS represented that all IHiS staff have been briefed to alert the SIRT or the SMD when a non-security IHiS staff encounters a suspicious incident. This was communicated to all IHiS staff through regular emails, circulars, wallpapers and intranet banners. IHiS also represented that insofar as the non-security IHiS staff are concerned, the general expectation was for them to report suspicious incidents to the SIRT or SMD. Such staff are not expected to be familiar with the details of the IT-SPS and SIRF, though these policies were made available via IHiS' intranet.

107 Given that IHiS regularly handles large volumes of sensitive personal data on behalf of the PHIs, the Commissioner finds that it is insufficient for IHiS to have merely informed its non-security staff to alert the relevant personnel through emails, circulars, wallpapers and intranet banners. These are effective in creating awareness amongst staff, but ineffective as policies for a number of reasons. Emails and circulars are disseminated and therefore

[42] The National Cyber Incident Response Framework is the framework for the reporting and management of cyber incidents affecting CIIs.

ineffective as a resource for future reference; while wallpapers and intranet banners are temporary and replaced eventually. The necessity of a set of written policies that are centrally stored (eg on the intranet) and which can be consulted cannot be replaced by these other means of creating awareness. IHiS had admitted that while the SIRF and IT-SPS were made available via IHiS' intranet, it had not developed any written policy on IT security incident reporting for its non-security staff. Furthermore, regular training sessions and staff exercises should have been conducted to ensure that all IHiS staff are familiar with the IT security incident reporting and their role in recognising and reporting suspected IT security incidents. These trio of awareness, training and written resource have to be deployed collectively for an effective staff training programme.

108 As the Commissioner observed in *Re SLF Green Maid Agency* [2018] SGPDPC 27 (at [13]), it is insufficient for organisations that handle large volumes of sensitive personal data to merely disseminate guidelines and instructions. It is necessary for the organisation to have a system of staff training and awareness:

> "For a company like the Organisation that handles personal data of foreign domestic workers and clients on a daily basis (eg passport and income information), it is **necessary for it to put in place a better system of staff training and awareness given the sensitive nature of personal data that it handles, as well as the volume**. **Merely disseminating guidelines and verbal instructions is insufficient**. As noted in *Re Aviva Ltd*, whilst there is no specific distinction in the PDPA based on the sensitivity of the data, organisations are to ensure that there are appropriate levels of security for data of varying levels of sensitivity: [2018] PDP Digest 245 at [17]-[18]. NRIC and passport numbers and financial information would generally be considered more sensitive: *Re Aviva Ltd* at [17]. **Structured and periodic training could have been implemented to protect personal data.**"
>
> [Emphasis added.]

109 Furthermore, the Commissioner finds that by IHiS' own admission, there were a number of vulnerabilities and gaps in SingHealth's network and in IHiS' systems and processes which were exploited by the attacker.

110 First, there were gaps in how IHiS' policies and practices were implemented and enforced, particularly in the management of the SGH Citrix Servers. IHiS asserts that its management gave clear directions and instructions to its Citrix Team Lead in July 2017 to turn on software firewall on the SGH Citrix Servers to block remote desktop protocol traffic from end-user workstations. However, firewall rules were not implemented on the SGH Citrix

Servers that were used by the attacker in the course of the attack. IHiS' staff failed to discharge their assigned responsibilities. IHiS had relied on its staff to follow through on instructions and the Citrix Team Lead to ensure that the instructions were complied with. In this case, however, both the team responsible for placing the firewalls and their supervisor, the Citrix Team Lead, failed to discharge their assigned responsibilities. To compound matters, IHiS updated the SingHealth CISO that the software firewall rules had been implemented without having verified this.

111 Second, there were insufficient steps taken to ensure that technical measures to protect personal data were carried out as intended and according to IHiS' own policies and practices. Such insufficiencies were exploited by the attacker.

112 *Weak local administrator passwords*: under the IT-SPS, administrator accounts were required to have a 15-character password. Notwithstanding, the local administrator account that the attacker relied on in the course of the attack had an easily deduced password ("P@ssw0rd") with only eight characters. The account also had the same password since 2012 despite the requirement for it to be changed every three to six months. Although IHiS had pushed its password policy and requirements through a Group Policy Object ("**GPO**"), which should apply to all servers by default, it did not apply to servers which had activated a setting to prevent the GPO from applying, such as the SGH Citrix Servers.[43]

113 In *Re Orchard Turn Developments Pte Ltd* [2017] SGPDPC 12, the Commissioner highlighted (at [35]) the importance of managing admin account credentials, and took the view that the implementation of an effective password expiry mechanism would have reduced the potential adverse impact of an unauthorised use of the admin account password:

> "On the facts, the **Organisation failed to put in place any formal policy or practice for the management of the admin account passwords to the EDM server**. Additionally, in terms of the Organisation's handling of the admin account credentials, the Commission identified two main areas of concern as follows:
>
> …
>
> (b) second, **the password of the admin account to access the EDM Application had not been changed since the roll out of the EDM**

[43] GPOs automate the implementation and enforcement of policies. They should apply to all servers by default, except for groups of servers which have the 'block policy inheritance' setting applied. Applying 'block policy inheritance' prevents group policies from being inherited from these servers. The SGH Citrix Servers were part of a group of servers which had group policy inheritance applied. As such, the GPOs implementing the complex password policy and policy for the deactivating of dormant accounts were not applied.

> **Application**, i.e. from November 2014 until the time of the data breach incident in December 2015. **The implementation of an effective password expiry mechanism would have reduced the potential adverse impact of an unauthorised use of the admin account password**."

[Emphasis added.]

114 *Passwords in cleartext was found in scripts*: the password of one of the local administrator accounts relied by the attacker in the course of the attack was found in cleartext in scripts on a SGH Citrix Server. This script was created by a Citrix Administrator despite specific instructions in March 2017 and June 2017 from his supervisors to clean up the scripts and avoid storing any passwords in the scripts in cleartext. Under the IT-SPS, passwords must not be stored as cleartext on storage systems, audit logs or when transmitted over the network but should configured to be encrypted, prompted or hashed.

115 In *Re The Cellar Door Pte Ltd*, the fact that login credentials were being transferred in clear and unencrypted text, which exposed the hosting environment to potential compromise should the credentials be intercepted, was found to be indicative of a poor level of security in the system design and implementation:[44]

> "In this case, the Respondents have failed to put such an all-round security in place. **The Commission has found several significant gaps in the security measures implemented as follow**:
> …
> (c) Login credentials were transferred in clear and unencrypted text. With regard to the Site's functionality, the Commission found that **login credentials (ie user logins and passwords) were being transferred in clear and unencrypted text, indicative of a poor level of security in the system design and implementation**. **This security vulnerability exposed the hosting environment to potential compromise should the credentials be intercepted**. Cellar Door, as the organisation having the overall responsibility and control over the design and functionalities of the Site, has the obligation to ensure that, as part of the design and functionalities of the Site, provisions were made for the security of the transmission of the login credentials. In its original design, the Site did not have such a security feature to protect the transmission of the login credentials – but this was prior to Section 24 of the PDPA coming into force on 2 July 2014. However, subsequently when the PDPA came into full effect on 2 July 2014, Cellar Door had the obligation to review the design and functionalities of the Site, and put in place the necessary security arrangements to comply with Section 24 of the PDPA. Yet, Cellar Door had failed to do so, and the Site still lacked in the necessary measures to secure the transmission of the login credentials."

[44] *Re The Cellar Door Pte Ltd* at [30].

[Emphasis added.]

116 *Dormant accounts were not disabled*: although IHiS' policies required a periodic review of unused or dormant accounts, the dormant local administrator account and service account relied on by the attacker in the course of the attack were not detected and disabled by IHiS because the automated process to detect and disable unused or dormant accounts only extended to "domain" accounts instead of local accounts.[45]

117 In *Re K Box Entertainment Group Pte Ltd and another* [2016] SGPDPC 1, the Commissioner found (at [26]) that the organisation had weak control over unused accounts. The organisation failed to make reasonable security arrangements to protect the personal data in its possession or under its control as it could have easily removed the unused accounts but it had failed to do so. As a result, the unused administrative account with a weak password ("admin") remained in the system and put the personal data of the organisation's members at risk:

> "In particular**,** the Commission has identified the following vulnerabilities in K Box's security arrangements which show how K Box failed to make reasonable security arrangements to protect the members' personal data:
>
> (b) **K Box had weak control over unused accounts, specifically, unused accounts were not removed:**
>
> (i) As stated at paragraph 14 above, as many as 36 accounts were removed from the CMS system on 17 September 2014, which suggests that K Box may not have had the practice of deleting the accounts of staff that had left the company until it conducted the review on 17 September 2014. This is despite the fact that K Box was able to remove the unused accounts within a day after the List had been disclosed online which shows that **K Box could have easily removed the unused CMS accounts earlier but it had failed to do so**;
>
> (ii) **As a result of K Box and/or Finantech's failure to promptly remove unused accounts from the CMS system, the unused administrative CMS account with the user name 'admin' and a weak password of 'admin' remained in the CMS for about one year after Mrs G had left Finantech**. **This had put the personal data of K Box's members at risk** because as noted at paragraph 20 above, Finantech itself had hypothesised that someone could have hacked into K Box's CMS using this 'admin' user account and planted a malware control and command centre to retrieve and export the members' data;"

[45] Domain accounts exist in the Microsoft Active Directory and are used to centrally manage servers and workstations within an enterprise when these computing resources join to a domain. In contrast, local accounts exist within each server or workstation and are not managed centrally.

[Emphasis added.]

118 *Lack of controls to detect bulk querying behaviour in the SCM database or queries being run from illegitimate client applications*: even though the SCM database contained sensitive personal data of millions of patients, there were no controls to detect bulk querying behaviour. However, IHiS represented that the use of such database access monitoring software or tools are not common in the healthcare sector and are generally only used in the security and banking/finance sector. The Public COI Report corroborates this.[46] As such, the Commissioner accepts that it was not unreasonable that IHiS did not have such controls in place at the material time.

119 That said, according to the Guide to Securing Personal Information issued by the Office of the Australian Information Commissioner ("**OAIC**"),[47] the use of proactive monitoring to identify possible unauthorised access or disclosure may be a reasonable step to take particularly if the organisation uses many systems or databases which hold large amounts of personal information:

> "**Audit logs, audit trails and monitoring access**
>
> Unauthorised access of personal information can be detected by reviewing a record of system activities, such as an audit log. Maintaining a chronological record of system activities (by both internal and external users) is often the best way for reviewing activity on a computer system to detect and investigate privacy incidents. Audit logs should also be named using a clear naming convention.
>
> Audit trails are used to reconstruct and examine a sequence of activities on a system that lead to a specific event, such as a privacy incident.
>
> **Access monitoring software that provides real time (or close to real time) dynamic review of access activity can also be useful for detecting unauthorised access to personal information**. **Use of proactive monitoring to identify possible unauthorised access or disclosure**, including any breach that might amount to an eligible data breach for the purposes of the NDB scheme, **may be a reasonable step for you to take particularly if you use many systems or databases which hold large amounts of personal information**."
>
> [Emphasis added.]

[46] Public COI Report at [221].
[47] Australia, OAIC, Guide to securing personal information: 'Reasonable steps' to protect personal information, June 2018 <https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information>.

120 In future, organisations that hold large amounts of personal data should consider implementation of database access monitoring as one of the security measures for early detection of unauthorised access or disclosure.

121 *Lack of controls to prevent or monitor communications between the SGH Citrix Servers and the SCM database at HDC*: such controls were only implemented after the unauthorised access from the SGH Citrix Servers to the SCM database was discovered. Even if it was necessary to keep a connection between the SGH Citrix Servers and the SCM database at HDC, such a connection should have been a protected connection and the servers using the connection should have been placed behind a firewall (which they were not). [48]

122 As highlighted in *Re The Cellar Door Pte Ltd*, *a* firewall is a fundamental measure that should be in place for servers to protect against an array of external cyber threats:[49]

> "In this case, the Respondents have failed to put such an all-round security in place. **The Commission has found several significant gaps in the security measures implemented as follow**:
>
> (a) No server firewall installed. While there was an alleged "software firewall configuration", there was no firewall installed to protect GIW's server itself at the material time. **A firewall is fundamental to the security of the server to protect against an array of external cyber threats, and GIW has the responsibility of ensuring that such a fundamental measure is in place for its server. In this case, a dedicated firewall (beyond the alleged software firewall configuration) protecting the server itself was only installed after the data breach incident had taken place.**"
>
> [Emphasis added.]

123 *Unpatched Microsoft Outlook email client maintained in the SingHealth IT environment*: the attacker was able to gain access to an unpatched end-user workstation running a version of Outlook by using a publicly available hacking tool. On this issue, IHiS submitted that it did not assess if an urgent roll-out to deploy the patch outside its usual patching cycle was required given that the patches released by Microsoft were not categorised as "Critical". In the circumstances, the Commissioner accepts that it was not unreasonable for IHiS to not have applied the patch at the material time. IHiS cannot be faulted for relying on the software

[48] As found at paragraph 1100 above.
[49] *Re The Cellar Door Pte Ltd* at [30].

provider's assessment of the criticality and urgency for applying the steady stream of updates and patches that are made available on a regular basis.

124 Notwithstanding, the Commissioner takes this opportunity to reiterate the importance of putting in place maintenance processes to ensure regular security patching as a security measure. Patching is one of the common tasks that all system owners are required to perform in order to keep their security measures current against external threats:[50]

> "First, **the Organisation failed to ensure regular patching of the EDM Application since its roll out** in November 2014. The KPMG Reports highlighted that the EDM Application was exposed to 24 known vulnerabilities because it did not follow a regular patching cycle. The KPMG also noted that the **EDM server appeared to have been patched in an ad-hoc manner once every two to four months. Patching is one of the common tasks that all system owners have to perform in order to keep its security measures current against external threats. The failure to patch the EDM Application regularly was a failure to protect the EDM Application against known system vulnerabilities**."
>
> [Emphasis added.]

125 For completeness, even though the SingHealth GCIO had oversight over the IHiS Delivery Group's administration and implementation of policies, seeing as the above vulnerabilities are basic operational tasks that fall within the type of day-to-day operations and technical support, maintenance and monitoring, which is managed by the IHiS Delivery Group, it was reasonable for SingHealth to have expected the IHiS Delivery Group to ensure that reasonable security arrangements which were within the scope of IHiS' responsibility were carried out.

126 Third, vulnerabilities that had previously been flagged out to IHiS were either not remediated or not addressed in time:

(a) IHiS was aware of some vulnerabilities in the Citrix Servers and had required its Citrix Team to fix the Citrix Servers to prevent exploitation. Although the Citrix Servers in H-Cloud were fixed, the same fixes were not applied to the SGH Citrix Servers, some of which were still in operation even though they were planned to be decommissioned;

[50] *Re Orchard Turn Developments Pte Ltd* at [38]. See also *Re The Cellar Door Pte Ltd* at [26].

(b) the GIA Audit Report had flagged out most of the vulnerabilities highlighted in paragraphs 110 to 123 above. Although IHiS had instructed its staff to address the vulnerabilities stated in the report, IHiS staff responsible for the remediation did not adequately track and ensure that all vulnerabilities were fully and properly remediated. Remediation was stated to be done when it was not actually done or not done thoroughly. No verification was conducted by IHiS line management. In particular, there was evidence that both IHiS and the GIA thought the implementation of firewall rules on the SGH Citrix Servers to block remote desktop protocol traffic from end-user workstations as a remediation measure had been completed by 7 August 2017[51] even though the team responsible for placing the firewall failed to discharge their assigned responsibilities (as observed at paragraph 110 above); and

(c) a coding vulnerability in the SCM application was flagged by a former IHiS employee in 2014 in an email sent to a competitor of Allscripts. Although the fact that there was a potential vulnerability in the SCM application was known to the management at IHiS at the time, no action was taken to investigate or remedy the vulnerability that he found. IHiS submitted that no action was taken at the time because it took the view that the vulnerability was not an issue, especially in light of its existing security measures and doubts over the credibility of their former employee. Allscripts had also been alerted to the possibility of a vulnerability. Pertinently, the SCM application is Allscripts' product. Allscripts did not inform IHiS of this apparent coding vulnerability and if this vulnerability will be remediated. It was not unreasonable for IHiS to assume that Allscripts would have issued a patch as part of its regular software support had they verified this apparent coding vulnerability. In view of this and the fact that the attacker could have used a different method to exploit the coding vulnerability in the SCM client application (that was likely also unknown to Allscripts at the time), which allowed the attacker to retrieve the SCM database login credentials from the H-Cloud Citrix Server, the Commissioner accepts that it was not unreasonable for IHiS to not have remedied the apparent coding vulnerability in the SCM application highlighted in 2014.

[51] At the SingHealth AC meeting held on 13 October 2017, GIA, which was in charge of ensuring that remediation measures were implemented and checked upon, stated that the implementation status of past audit issues was largely on track. According to the IHiS Delivery Group, the specific remediation measure of network segregation enhancement had already been completed.

127 Fourth, even though IHiS represented that it had communicated to all IHiS non-security staff through regular emails, circulars, wallpapers and intranet banners that the SIRT or SMD should be alerted whenever they encounter a suspicious incident, the fact that IHiS employees who first encountered the suspicious activity failed to escalate it to the SIRT, as opposed to notifying an individual who happened to be part of the SIRT, suggests that the approach adopted by IHiS (where there was no written IT security incident policy in place and no training) was inadequate and IHiS non-security staff did not have a good understanding of the importance and requirements for reporting IT security incidents. The SIRM also failed to comply with the SIRF and IR-SOP.[52]

128 In January 2018, when the SIRM was alerted to call-backs to a suspicious foreign IP address from the workstations compromised by the attacker, he did not take steps to block that IP address for the entire SCM network, or initiate any investigations, which could have identified and contained the compromised workstations before they were eventually used in the attack, including a compromised workstation which was eventually used as a means of exfiltration ("**January 2018 incident**"). The SIRM failed to escalate the January 2018 incident as he took the position (which IHiS did not endorse) that this was not a reportable incident as it pertained to a malware infection that had been detected and cleaned without network propagation. In fact, the SIRM did not make any effort to determine whether there had been any such network propagation.

129 From mid-June 2018, when IHiS staff had identified multiple failed login attempts to the SCM database originating from the compromised SGH Citrix Servers, using invalid credentials, or accounts that had insufficient privileges, the SIRM failed to escalate or take any additional steps to manage the vulnerabilities, as he was labouring under the misapprehension that a cybersecurity incident should only be escalated when it is "confirmed". The SIRM failed to appreciate that timely incident reporting, in accordance with the relevant IHiS policies and standards on incident reporting, could enable more resources to be deployed to better investigate and contain a cybersecurity incident.[53]

---

[52] In this regard, the Public COI Report also highlighted (at [926] and [927]) that even within the IHiS SMD, the processes for reporting observations were inconsistent and unclear. There was no established procedure for how IHiS staff should escalate a matter internally or how to report a security incident to the SingHealth CISO or the SingHealth GCIO. This resulted in confusion and consequent delays in response.

[53] The COI also found at ([433] and [593]) that he had delayed reporting because he felt that additional pressure would be put on him and his team once the situation became known to management. The evidence also suggested

130 As highlighted in *Re National University of Singapore* [2017] SGPDPC 5, data protection policies and practices are only effective when staff understand and are familiar with the policy and put its security procedures in practice:[54]

> "In another case, the Office of the Privacy Commissioner of Canada ("**OPC**") explained that whilst security policies and procedures are essential, they are not in themselves sufficient to protect personal information; **the effectiveness of security safeguards depends on the organisation's**:
>
> > ***"[d]iligent and consistent execution of security policies and procedures [which] depends to a large extent on ongoing privacy training of staff and management, so as to foster and maintain a high organizational awareness of informational security concerns".***
>
> In a separate investigation, the OPC further clarified its position and stated that security policies and practices are only effective when "*properly and consistently implemented and followed by employees*"."
>
> [Emphasis added.]

131 However, it was apparent from the response of a number of IHiS staff and in particular, the SIRM's response, that the communications and training provided to them was inadequate for them to fully comprehend and internalise the existing framework and SOPs.

132 To be clear, the PDPA does not require organisations to provide an *absolute guarantee* for the protection of the personal data in its possession or under its control. As the Commissioner clarified in *Re Tiger Airways & Ors.* [2017] SGPDPC 6 (at [17]): [55]

> "In the context of section 24, this means that **an organisation is not required to provide an absolute guarantee for the protection of personal data in its possession**, but that it **must make such security arrangements as a reasonable person would consider appropriate, given the nature of the personal data involved and the particular circumstances of that organisation**."
>
> [Emphasis added.]

133 Even so, in consideration of the facts and circumstances surrounding the Data Breach, the Commissioner finds that IHiS had not done what a reasonable person would consider appropriate to prevent the unauthorised exfiltration of the personal data in the SCM database.

---

that the reluctance to escalate potential security incidents may have come from a belief that it would not reflect well in the eyes of the organisation if the matter turned out to be a false alarm.

[54] *Re National University of Singapore* at [24] and [25].

[55] See also *Re BHG* at [25].

In view of the very large volume of sensitive medical personal data managed and processed by IHiS on behalf of SingHealth, it is reasonable to expect IHiS to accord SingHealth's IT systems and, in particular, the SCM database a higher standard of protection. However, by IHiS' own admission, the weaknesses, lapses and failures on the part of some IHiS personnel to comply with IHiS' security framework showed that the administrative or organisational security measures that IHiS had in place at the time of the Data Breach were inadequate.

134 Accordingly, even though IHiS had in place a number of security arrangements to protect the personal data in its possession or under its control, the Commissioner finds that IHiS had not taken sufficient security steps or arrangements to protect the personal data in the SCM database from unauthorised access, collection, use, disclosure and copying.

Directions

135 Having considered the evidence obtained by the Commission during its investigation and the representations of the parties, the Commissioner is satisfied that both SingHealth and IHiS have breached section 24 of the PDPA. The Commissioner is empowered under section 29 of the PDPA to give such directions as he deems fit to ensure compliance with the PDPA.

136 The Commissioner hereby directs SingHealth to pay a financial penalty of $250,000 within 30 days of the issuance of this direction, failing which interest at the rate specified in the Rules of Court in respect of judgment debts shall accrue and be payable on the outstanding amount of such financial penalty until the financial penalty is paid in full.

137 The Commissioner hereby directs IHiS to pay a financial penalty of $750,000 within 30 days of the issuance of this direction, failing which interest at the rate specified in the Rules of Court in respect of judgment debts shall accrue and be payable on the outstanding amount of such financial penalty until the financial penalty is paid in full.

138 The financial penalties imposed against the two Organisations are individually the highest and second highest financial penalty amounts imposed by the Commission to date. This is appropriate given the circumstances.

139 First, this is the largest data breach suffered by any organisation in Singapore with the number of affected individuals amounting to almost 1.5 million unique individuals. Second,

while the attacker managed to exfiltrate the personal data of almost 1.5 million unique individuals, the SCM database which was attacked contained patient data belonging to over 5.01 million unique individuals whose personal data was put at risk. This increases the seriousness of IHiS and SingHealth's data security inadequacies. The patient data held in the SCM database contained highly sensitive and confidential personal data including clinical episode information, clinical documentation, patient diagnosis and health issues and Dispensed Medication Records. It is not difficult to imagine the potential embarrassment that a patient may suffer if such sensitive information about the patient and the patient's health concerns were made known to all and sundry. As such, it is critical for the Organisations to protect the security and confidentiality of such medical records. Third, the attacker exfiltrated the Dispensed Medication Records of 159,000 unique individuals together with the Patient Particulars. From the Dispensed Medication Records, one may be able to deduce the condition for which a patient was being treated. This may include serious or socially embarrassing illnesses.

SingHealth's Representations

140 SingHealth made representations for a reduction in the quantum of the financial penalty as set out in the preliminary Decision on the basis that the Commission should factor in the principle of proportionality in deciding the appropriate financial quantum and the extent to which SingHealth had failed to discharge its obligations. In this regard, SingHealth represented that they did have in place various security measures which were reasonable to have oversight of its data intermediary except in relation to the lapses of an individual.

141 The fact that an organisation has adequately implemented other protection policies will not operate to absolve or mitigate liability for breaches. In *Re Funding Societies Pte Ltd* [2018] SGPDPC 29, the organisation pleaded in mitigation that it had in place "a framework of security arrangements, such as a risk management framework, an information security policy and training and audits of its policies and procedures." In response, the Commissioner stated:[56]

> "Neither should **the fact that the Organisation continuously assessed its compliance with the obligations set out in the PDPA and that it had the necessary frameworks in place mitigatory as these were the standard of conduct expected for compliance**. These are not activities or measures which

[56] *Re Funding Societies Pte Ltd* at [32] and [33].

> go beyond the standard of protection required by the PDPA and as such is not a mitigating factor."
>
> [Emphasis added.]

142 Even in cases where both the organisation and data intermediary have been found to be in breach of the PDPA, the Commissioner will assess each party's breach on its own merits and circumstances. In calculating the quantum of the financial penalty to be imposed, the Commissioner takes an objective approach in assessing the facts and circumstances of the contravention and how a reasonable organisation or data intermediary should have behaved in the circumstances. In this regard, as explained in the Advisory Guidelines on Enforcement of the Data Protection Provisions (issued 21 April 2016) (at [25.2]), one of the factors that the Commission may consider to be an aggravating factor includes:

> "the organisation is **in the business of handling large volume of sensitive personal data, the disclosure of which may cause exceptional damage, injury or hardship to a person (such as medical or financial data), but failed to put in place adequate safeguards proportional to the harm that might be caused by disclosure** of that personal data."
>
> [Emphasis added.]

143 Nevertheless, in assessing the breach and determining the directions to be imposed on SingHealth, the Commissioner took into account the following mitigating factors:

(a) SingHealth voluntarily and unequivocally admitted to the facts, accepted the Commission's findings set out in this Decision and had agreed to cooperate with the Commission to expedite the Investigation and the determination of liability for each of the parties and issue any directions that the Commission deems fit;

(b) SingHealth was constrained, in that, as a matter of policy, all IT functions and capabilities for the public healthcare sector (including the proposed structure and resourcing for the SingHealth GCIO Office) are centralised in IHiS;

(c) SingHealth was cooperative during the Investigation;

(d) SingHealth took immediate effective remedial action following the Data Breach; and

(e) SingHealth was as much a victim of the malicious actions of a skilled and sophisticated threat actor who used advanced methods that overcame enterprise security measures as the individuals whose personal data was illegally accessed and copied.

144 Similarly, in assessing the breach and determining the directions to be imposed on IHiS, the Commissioner took into account the following mitigating factors:

(a) IHiS voluntarily and unequivocally admitted to liability and had agreed to cooperate with the Commission to expedite the Investigation and the determination of liability for each of the parties and issue any directions that the Commission deems fit;

(b) IHiS was cooperative during the Investigation;

(c) IHiS took immediate effective remedial action following the Data Breach; and

(d) IHiS was as much a victim of the malicious actions of a skilled and sophisticated threat actor who used advanced methods that overcame enterprise security measures as the individuals whose personal data was illegally accessed and copied.

145 Without the above mitigating factors, the Commissioner would have imposed the maximum financial penalty allowed under the PDPA against IHiS and a financial penalty at a significantly higher quantum against SingHealth.

146 The Commissioner has not set out any further directions for IHiS and SingHealth given the remediation measures already put in place.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR COMMISSIONER FOR PERSONAL DATA PROTECTION