Capitol Health Limited

ACN 117 391 812

Notifiable Data Breaches Policy

TABLE OF CONTENTS

1. Purpose

This Notifiable Data Breaches Policy (**Policy**) establishes the requirements for Capitol Health Limited (**Capitol**) in responding to data breaches under the Notifiable Data Breaches (**NDB**) Scheme under Part IIIC of the Australian Privacy Act 1988 (Cth) (**Privacy Act**). Capitol has data breach notification obligations when a data breach is likely to result in serious harm to any individuals whose personal information is involved in the breach.

2. Application of the Policy

The NDB scheme applies to Capitol as an 'APP entity'- an organisation with existing personal information security obligations under the Privacy Act.

3. Overview

Capitol has data breach notification obligations when a data breach is likely to result in serious harm to any individuals whose personal information is involved in the breach. This notification must include recommendations about the steps individuals should take in response to the breach. The Australian Information Commissioner (**Commissioner**) must also be notified of eligible data breaches.

4. What is an eligible data breach?

An 'eligible data breach' arises when the following three criteria occur:

- unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information;
- that is likely to result in serious harm to one or more individuals; and
- Capitol has not been able to prevent the likely risk of serious harm with remedial action.

Examples of a data breach include when:

- a device containing customers' personal information is lost or stolen
- a database containing personal information is hacked
- personal information is mistakenly provided to the wrong person

5. Which data breaches require notification?

An 'eligible data breach' that triggers notification obligations, is a data breach that is likely to result in 'serious harm' to any of the individuals to whom the information relates.

What is 'serious harm'?

Serious harm may include serious physical, psychological, emotional, financial, or reputational harm.

Relevant matters to assist the assessment of serious harm include:

- kind of information
- sensitivity of the information
- if the information is protected by one or more security measures
- kind/s of person/s who have obtained, or who could obtain the information
- if a security technology or methodology was used in relation to the information and was designed to make the information unintelligible or meaningless to persons not authorised to obtain the information
- the kind/s of person/s who have obtained or who could obtain the information, who may have intentions of causing harm and to circumvent the security technology or methodology
- nature of the harm

Types of personal information involved in the data breach

Some kinds of personal information may be more likely to cause an individual serious harm if

compromised, including:

- sensitive information about health
- documents commonly used for identity fraud (Medicare card, driver licence, passport)
- financial information
- combination of types of personal information allowing more to be known about individuals

Circumstances of data breach

The specific circumstances of the data breach are relevant when assessing whether there is a risk of serious harm to an individual including:

- Whose personal information was involved in the breach? Some individuals are more vulnerable increasing the risk of serious harm
- How many individuals were involved? The scale of the breach affects the likelihood of risks
- Do the circumstances of the data breach affect the sensitivity of the personal information
- How long has the information been accessible?
- Is the personal information adequately encrypted, anonymised, or not easily accessible?
- What parties may/ have gained unauthorised access to the personal information intended for malicious purposes

6. Data breaches involving more than one organisation

Where Capitol holds personal information jointly with other entities, an eligible data breach of one entity will also be an eligible data breach of the other entities. Compliance by one entity is taken as compliance by each of the entities holding the information.

Where multiple entities jointly hold information compromised in a data breach, only one entity needs to take the steps required by the NDB scheme. The Privacy Officer will decide which one, however the entity with the most direct relationship with the affected individuals should undertake the notification.

When is information held jointly

Personal information is held when there is possession or control of a record that contains personal information. This extends beyond the physical possession, to include records that Capitol has a right or power to deal with, even if it does not physically possess the record or own the medium on which it is stored.

Capitol holds records with cloud service providers, outsourcing entities, shared services agreements, Commonwealth contracts and joint ventures. As Capitol has contractual rights to retain control of the records (rights to access and use the records), all entities hold the information.

Responding to data breaches of jointly held information

Where Capitol holds the same record of personal information with another entity, both entities are responsible for complying with the NDB scheme in relation to that record.

Only one of the entities that jointly holds information needs to comply with the NDB scheme's assessment and notification requirements on behalf of the group. If no assessment is conducted each entity holding the information may be found to be in breach of the assessment requirements.

Only one entity needs to notify individuals and the Commissioner if there is an eligible data breach involving personal information jointly held by more than one entity (Identifying eligible data breaches). Whether a data breach is likely to result in serious harm requires an objective assessment, determined from the viewpoint of a reasonable person in the entity's

position. If none of the entities notify, then all may be found to have breached the notification requirements of the NDB scheme.

7. Preventing serious harm with remedial action

If a data breach is positively addressed by remedial action in a timely manner, and the outcome is not likely to result in serious harm, then the breach is not an eligible data breach therefore avoiding the need to notify. For breaches where information is lost, the remedial action is adequate if it prevents unauthorised access to, or disclosure of personal information.

If the remedial action prevents the likelihood of serious harm to some individuals within a larger group of individuals whose information was compromised, notification to those individuals for whom harm has been prevented is not required.

8. Allocation of responsibility for compliance

Capitol demonstrates the meeting of the NDB Scheme requirements through the tailoring of arrangements with contractual and customer relationships.

Where information is held jointly, Capitol has clear procedures for complying with the NDB Scheme, when entering into service agreements and other relevant contractual arrangements. This includes obligations around the communication of suspected breaches, processes for conducting assessments, and responsibility for containment, remediation, and notification.

9. Assessing a suspect data breach

Where Capitol suspects or becomes aware that an eligible data breach may have occurred a reasonable and expeditious assessment will be undertaken to determine if the data breach is likely to result in serious harm to any individual affected. Where an eligible data breach has occurred, Capitol will promptly notify individuals at risk of serious harm and the Commissioner.

All reasonable steps to complete the assessment within 30 calendar days after the day Capitol becomes aware of the suspected eligible data breach will be taken. Capitol will endeavour to complete the assessment in a shorter timeframe as the risk of serious harm to individuals may increase with time.

Where Capitol cannot reasonably complete an assessment within 30 days, documentation will be provided to the Commissioner to demonstrate:

- all reasonable steps have been taken to complete the assessment within 30 days
- reasons for the delay
- the assessment was reasonable and expeditious.

Capitol has practices, procedures, and systems in place to comply with information security obligations under APP 11, enabling suspected breaches to be promptly identified, reported to relevant personnel and assessed.

10. Capitol Data Breach Response Plan

This Response Plan enables Capitol to contain, assess and respond to any data breaches in a timely fashion, help mitigate potential harm to affected individuals and assist in mitigating costs. At all times steps will be taken to reduce any potential harm to individuals caused by a suspected/ eligible data breach.

Responding to data breaches of jointly held information

All suspected eligible data breaches must be notified via the following e-mail

privacy@capitolhealth.com.au which will bring the notification to the attention of the Privacy Officer as soon as possible after a suspected eligible data breach has occurred.

Data Breach Response Team

The Data Breach Response Team (**Response Team**) consists of the Chief Executive Officer (CEO), Chief Financial Officer (CFO), Company Secretary and Head of IT. Other Capitol employees will be involved as required. Minor data breaches may be dealt with without action from the Response Team.

The Privacy Officer will use his/ her discretion to determine whether a suspected/ data breach requires escalation to the Response Team, considering the following questions:

- are multiple individuals affected?
- is there, or may there be real risk of serious harm to affected individual/s?
- does the suspected/ breach indicate a systemic problem in Capitol' processes and procedures?
- could there be media or stakeholder attention as a result of the suspected/ breach?

If the answer to any of these questions is 'yes', the Privacy Officer will notify the Response Team.

Where the Privacy Officer decides not to escalate a minor suspected/ data breach to the Response Team he/ she will send an email to the CEO containing:

- description of the action taken by the Coordinator in managing the suspected/ breach
- the outcome of that action
- the Privacy Officer's view that no further action is required

11. Individuals and the Commissioner

When Capitol becomes aware that an eligible data breach has occurred the Privacy Officer will promptly organise the notification of individuals at likely risk of serious harm, where serious harm cannot be mitigated through remedial action.

The Privacy Officer will also notify the Commissioner as soon as practical through a statement about the eligible data breach.

If it is not practical to notify individuals at risk of serious harm, Capitol will publish a copy of the statement prepared for the Commissioner on the website, and take reasonable steps to bring its contents to the attention of individuals at risk of serious harm.

There are three options for notifying individuals at risk of serious harm, depending what is practical and what capacity Capitol has.

Option 1 — Notify all individuals

If practical Capitol can notify each of the individuals whose personal information was part of the eligible data breach if it cannot be reasonably assessed which particular individuals are at risk of serious harm from the eligible data breach. Where risk of serious harm is likely for one or more of the individuals, all individuals are to be notified.

Option 2 — Notify only those individuals at risk of serious harm

Where Capitol identifies that only a particular individual or a specific subset of individuals are at risk of serious harm, only those individuals need to be notified. This is to avoid unnecessary distress to individuals who are not at risk and reduces administrative costs.

Option 3 – Publish notification

If neither option 1 or 2 above are practical Capitol will:

- prominently place a copy of the statement on the website where it is easily located by

individuals and indexed search engines
- take reasonable steps to publicise the contents of the statement on relevant social media channels, print or online advertisement or relevant publications

to increase the likelihood that the eligible data breach will come to the attention of individuals at risk of serious harm. This information will be kept available for at least 6 months.

How to notify and what to say
Any reasonable method to notify individuals, including telephone call, SMS, physical mail, social media, personal conversation, nominated intermediary is acceptable.

Notification can be tailored to individuals, as long as it includes the content of the statement prepared for the Commissioner.

Timing of notification
Capitol will notify individuals as soon as practical after completing the statement notifying the Commissioner. Individuals will be notified of the contents of the statement given to the Commissioner. Notification to affected individuals can be before, or at the same time as notifying the Commissioner.

Identify and contact details
Where an entity's company name is different to the business or trading name the notifying entity will also include the name most familiar to individuals and how they can contact it. Depending on the nature and scale of the breach a dedicated phone line or email address to answer queries from individuals may be established.

Statement to the Commissioner
The statement will include sufficient information about the data breach to allow affected individuals to properly assess the possible consequences for them, and to take protective action in response.

Information describing the eligible data breach will include:
- Capitol's contact details
- description of the eligible data breach
- kind/s of information involved in the eligible data breach
- date/ range of the unauthorised access or disclosure
- date the entity detected the data breach
- Circumstances/ known cause of the data breach
- general description who has/ likely to have obtained access to the information
- steps taken to contain or remediate the breach
- recommended steps individuals should take in response to the eligible data breach

Where additional relevant information becomes available after submitting the statement, this may be provided to the Office of the Australian Information Commissioner (**OAIC**).

The statement of notification to the Commissioner can be made using the OAIC's Notifiable Data Breach form.

The Privacy Officer may provide additional supporting information to the Commissioner which may not be appropriate to include in the statement to individuals. This information assists the Commissioner to make further inquiries or to take any other action. Capitol can elect that additional supporting information provided to the Commissioner be held in confidence.

Regulatory action may be taken by the Commissioner in response to a notification. Generally, the Commissioner's priority when responding to notifications is to provide guidance and assist individuals at risk of serious harm.

Steps recommended to individuals in response to the eligible data breach

Recommendations will be prepared and provided by the Privacy Officer and include practical steps that are easy for affected individuals to action. Recommendations will depend on the circumstances of the eligible data breach and the kind/ s of information involved.

The Commissioner's enforcement of the NDB Scheme

If the Commissioner and Capitol cannot agree about whether notification should occur, the Commissioner will give Capitol an opportunity to make a well-reasoned and convincing formal submission about why notification is not required, or if notification is required, on what terms. Detailed evidence or information in support of this must be provided.

The Commissioner may declare that notification of a particular data breach is not required or the period in which notification needs to occur can be modified. This will occur once the Commission is satisfied that it is reasonable in the circumstances to do so, having regard to the public interest, any relevant advice received from an enforcement body or the Australian Signals Directorate and any other relevant matter.

12. Review/Evaluation

After the Response Team has completed their full investigation of the eligible data breach, a prevention plan will be instituted, audits conducted to ensure the plan is implemented, security/ response plan updated, appropriate changes to policies and procedures made and a revision of staff training practices. Refer to the OAIC's Guide to securing personal information.

13. Variations

This Notifiable Data Breaches Policy is effective from 21 June 2018.

The Capitol Board has reviewed the Policy on 23 March 2022 and it reserves the right to vary, replace or terminate this Policy from time to time.