9. Management of Data Breach Policy and Procedure

Approval Date: 20 Jan 2020	**Review date:** 20 Jan 2021	**Version:** 1.0

Purpose

To meet legislative compliance requirements as a mandatory reporter of eligible data breaches to both the Office of the Australian Information Commissioner (OAIC) and any individuals who may be potentially affected by a data breach; to inform relevant authorities of any breach; and to limit and reduce risks to the business and ensure continuous improvement in maintenance of data held by our organisation.

Scope

All staff are required to maintain the confidentiality of all data relating to participants and other staff members.

This policy relates to all personal data regarding both participants and team members.

Definition

Terminology	Description
Data Breach (Eligible Data Breach)	• Unauthorised access to or unauthorised disclosure of personal information or personal information is lost in circumstances where unauthorised access to, or unauthorized disclosure of the information is likely to occur. • *A reasonable person* would conclude that the access or disclosure would be *likely to result in serious harm* to any of the individuals to whom the information relates.
Likely (likely to result in serious harm)	Is to be interpreted to mean more probable than not
Reasonable Person	Is to be taken to mean a person in Australian Quality Care who is properly informed, based on information immediately available or following reasonable inquiries or an assessment of the data breach.

	OAIC's guidance states that the reasonable person is not to be taken from the perspective of an individual whose personal information was part of the data breach or any other person, and, generally, entities are not expected to make external enquiries about the circumstances of each individual whose information is involved in the breach.
Likely to result in serious harm – **Potential forms of serious harm**	An assessment as to whether an individual is likely to suffer 'serious harm' because of an eligible data breach depends on, among many other relevant matters: ● The kind and sensitivity of the information subject to the breach ● Whether the information is protected and the likelihood of overcoming that protection ● If a security technology or methodology is used in relation to the information to make it unintelligible or meaningless to persons not authorised to obtain it - the information or knowledge required to circumvent the security technology or methodology ● The persons, or the kinds of persons, who have obtained, or could obtain, the information; and ● The nature of the harm that may result from the data breach which could include physical, psychological, emotional, economic and financial harm as well as harm to reputation.
Remedial action	There are a number of exceptions to the notification obligation, including importantly where an entity is able to take effective remedial action to prevent unauthorised access to, or disclosure of, information when it is lost or to prevent any serious harm resulting from the data breach. Where such remedial action is taken by an entity, an eligible data breach will not be taken to have occurred, and therefore an entity will not be required to notify affected individuals or the OAIC

Suspicion of an eligible data breach	If Australian Quality Care merely *suspects* that an eligible data breach has occurred, but there are no reasonable grounds to conclude that the relevant circumstances amount to an eligible data breach, the entity must undertake a "reasonable and expeditious assessment" of whether there are in fact reasonable grounds to believe that an eligible data breach has occurred
Assessment time frame	Within 30 days after the day, it became aware of the grounds that caused it to suspect an eligible data breach.
Personal Information	Personal information includes a broad range of information, or an opinion, that could identify an individual. What is personal information will vary, depending on whether a person can be identified or is identifiable in the circumstances. For example, personal information may include: ● An individual's name, signature, address, phone number or date of birth ● Sensitive information ● Credit information ● Staff member record information ● Photographs ● Internet protocol (IP) addresses ● Voiceprint and facial recognition biometrics (because they collect characteristics that make an individual's voice or face unique) ● Location information from a mobile device (because it can reveal user activity patterns and habits) Does not cover people who have died.

Policy

Australian Quality Care views data breaches as having serious consequences, so the organisation must have robust systems and procedures in place to identify and respond effectively.

Australian Quality Care will delegate relevant staff members with the knowledge and skills required to become a Response Team member.

Staff are required to inform the Board or their delegate of the potential, or suspected, data breach immediately. Within forty eight (48) hours, the Board is to complete an electronic Notifiable Data Breach Form on the Office of the Australian information Commissioner webpage and ensure that, as a regulated entity, they notify the particular individuals and the Commissioner about eligible data breaches as soon as practicable (no later than thirty (30) days after becoming aware of the breach or suspected breach).

If a Staff member becomes aware that there are reasonable grounds to believe that there has been an *notifiable data breach*, Australian Quality Care are required to promptly notify any individuals at risk of being affected by the data breach and the OAIC.

Australian Quality Care will undertake the following when an eligible data breach has occurred:

1) Prepare a statement that, at a minimum, contains:
    a) Australian Quality Care contact details:
        i) If relevant, the identity and contact details of any entity that jointly or simultaneously holds the same information, in respect of which the eligible data breach has occurred, e.g. due to outsourcing, joint venture or shared services arrangements. If information of this sort is included in the statement, the other entity will not need to report the eligible data breach separately
    b) A description of the data breach
    c) The kinds of information concerned
    d) The steps it recommends individuals take to mitigate the harm that may arise from the breach (while the entity is expected to make reasonable efforts to identify and include recommendations, it is not expected to identify every recommendation possible following a breach).
2) Provide a copy of the prepared statement to the OAIC using online Notifiable Data Breach Form
3) Undertake such steps, as are reasonable in the circumstances, to notify affected or at-risk individuals of the contents of the statement. Individuals will be notified by email, telephone or post, depending on the situation. If direct notification is not practicable Australian Quality Care will publish the statement on its website and take reasonable steps to publicise its contents.

Procedure

Stage 1 - Assess and determine the potential impact

- Once notified of the potential data breach, the General Manager must consider whether a privacy data breach has (or is likely to have) occurred and then make a preliminary judgement as to its possible severity. Advice on how to manage the data breach should be sought from appropriate managerial Staff.
- Criteria for determining whether a privacy data breach has occurred:
    - Is personal information involved?
    - Is the personal information of a sensitive nature?
    - Has there been unauthorised access to personal information, or unauthorised disclosure of personal information or loss of personal information, in circumstances where access to the information is likely to occur?
- Criteria for determining the severity of the breach:
    - Type and extent of personal information involved
    - Number of individuals that have been affected
    - If information is protected by any security measures (password protection or encryption)
    - Type of person/s who now have access
    - Whether there is (or could be) a real risk of serious harm to the affected individuals
    - If there could be media or stakeholder attention due to the breach/suspected breach.
- With respect to the above, serious harm could include physical, physiological, emotional, economic/financial or harm to reputation and is defined in Section 26WG of the Privacy Amendment (Notifiable Data Breaches) Act 2017

AQC will take a preliminary view as to whether the breach (or suspected breach) may constitute a Notifiable Data Breach.

Stage 2 - Select appropriate data breach management option

Option 1 - Data breach managed at a local level by managerial staff

1. The Board or their delegate will ensure implementation of immediate corrective action, if this has not already occurred. Corrective action may include retrieval or recovery of the personal information, ceasing unauthorised access, shutting down or isolating the affected system.
2. A Data Breach Process Report is to be completed within 48 hours of receiving instructions. The report will contain the following:
    - Description of the breach or suspected breach
    - Summary of action taken

- Summary of outcomes from the action taken
- Outline of processes implemented to prevent a repeat situation
- Recommendation outlining why no further action is necessary.

3. The Board or their delegate will sign-off, confirming that no further action is required.

Option 2 - Data breach managed by the Data Breach Response Team

1. When the Board or their delegate instructs that the data breach be escalated to the Response Team, the Board or their delegate will convene the Response Team and notify any relevant managerial Staff.
2. The Response Team will consist of:
    - General Manager
    - Human Resources (or nominee)
    - Information Technology (or nominee)
    - Marketing and external relations (or nominee)
    - Other person/s nominated by the Board or their delegate

Primary role of the Data Breach Response Team

There is no single method of responding to a data breach. Each incident must be dealt with, on a case by case basis, by assessing the circumstances and associated risks to inform the appropriate course of action.

The following steps may be undertaken by the Response Team, as appropriate:

1. Immediately contain the breach if this has not already occurred. Corrective action may include retrieval or recovery of the personal information, ceasing unauthorised access, shutting down or isolating the affected system.
2. Evaluate the risks associated with the breach, including collecting and documenting all available evidence of the breach, having regard for the information outlined above.
3. Call upon the expertise of, or consult with, relevant Staff in specific circumstances.
4. Engage independent cybersecurity or a forensic expert, as appropriate.
5. Assess whether serious harm is likely (with reference above and to Section 26WG of the Privacy Amendment (Notifiable Data Breaches) Act 2017.
6. Make a recommendation to the Board or their delegate whether this breach constitutes an NDB for mandatory reporting to the OAIC; and the practicality of notifying affected individuals.
7. Consider developing a communication or media strategy including the timing, content and method of any announcements to participants, Staff or the media.
8. The Response Team must undertake its assessment within 48 hours of being convened.

Secondary role of the Data Breach Response Team

Once the data breach has been dealt with appropriately, the Response Team should turn its attention to the following steps:

1. Identify lessons learnt and remedial action that can be taken to reduce the likelihood of a recurrence; this may involve a review of policies, processes and refresher training.
2. Prepare a report for submission to senior management.
3. Consider conducting an audit to ensure that necessary outcomes are affected and effective.

Stage 3 - Notify the Office of the Australian Information Commissioner

- Taking into consideration the Response Team's recommendation, the Board or their delegate will determine whether there are reasonable grounds to suspect that a Notifiable Data Breach has occurred.
- If there are reasonable grounds, the Board or their delegate must prepare a prescribed statement and provide a copy to the OAIC as soon as practicable (and no later than 30 days after becoming aware of the breach or suspected breach).

Relevant documents

- Data Breach Process_Form-1043
- Notifiable Data Breach

References

- NDIS Practice Standards and Quality Indicators 2020 – Version 3
- Privacy Act (1988)
- Privacy Amendment (Notifiable Data Breaches) Act 2017