ST LOUIS DATA BREACH RESPONSE POLICY AND DATA BREACH RESPONSE PLAN

Subject:	Data breach response policy and data breach response plan
Standard 8:	Organisational Governance
Expected outcome:	Information Management (3c)
Developed:	February 2018
Review date:	January 2021 by Administrator

1 Purpose of policy

1.1 We are committed to implementing and maintaining reasonable security safeguards and taking reasonable steps to protect the personal information we hold from misuse, interference and loss, and from unauthorised access, modification or disclosure.

1.2 If personal information is lost or subjected to unauthorised access, modification, use or disclosure, or other misuse or interference, then a data breach has occurred.

1.3 The purpose of this policy and procedure is to:

(a) set out the process we will follow if a data breach occurs;

(b) minimise the risk of serious harm to individuals which may result from a data breach;

(c) comply with our obligations in relation to managing eligible data breaches;

(d) ensure Workers understand their obligations and responsibilities.

2 Scope

This policy applies to employees, contractors or subcontractors, employees of a labour hire company assigned to work in our business, outworkers, apprentices or trainees, work experience students and volunteers (**Workers**).

3 Our obligations and responsibilities

3.1 Security of personal information

We are required to take reasonable steps to protect the personal information we hold from misuse, interference and loss and from unauthorised access and disclosure.

Details about how we manage personal information is set out in our Privacy Policy.

3.2 Notification of Eligible Data Breaches

(a) An Eligible Data Breach happens if:

(i) there is unauthorised access to, unauthorised disclosure of, or loss of, personal information held by an entity; and

(ii) the access, disclosure or loss is likely to result in serious harm to any of the individuals to whom the information relates.

(b) We must notify the affected individual(s) or organisation(s) (**affected individuals**) **and** the Office of the Australian Information Commissioner (**OAIC**) if:

(i) we have reasonable grounds to believe that an eligible data breach has happened; or

(ii) we are directed to do so by the OAIC.

4 Obligations of Workers

4.1 All Workers are responsible for reporting an actual or suspected data breach to the Privacy Officer.

4.2 The Privacy Officer is responsible for taking immediate steps in accordance with the Data Breach Response Plan (Annexure 1) including:

(a) recording the reported breach using Part A of the Data breach report form (Annexure 3);

(b) taking immediate steps to contain the breach; and

(c) notifying the Director of Care.

4.3 The Service Manager is responsible for investigating, assessing and responding to the data breach in accordance with the *Data breach response plan* (Annexure 1) including:

(a) completing the *Data breach matrix* (Annexure 2);

(b) completing Part B of the *Data breach report form* (Annexure 3);

(c) notifying the Administrator;

(d) determining whether the breach is required to be notified and if so, ensuring the relevant parties are notified.

5 Eligible data breach

5.1 What is an Eligible Data Breach?

The obligation to notify the OAIC and affected individuals only applies if there has been an Eligible Data Breach.

Not all data breaches will be an Eligible Data Breach.

An Eligible Data Breach occurs when a reasonable person would conclude that there is a likely risk of serious harm to any of the affected individuals as a result of the unauthorised access, unauthorised disclosure or loss.

5.2 What is serious harm?

Serious Harm can include:

(a) physical harm;

(b) psychological harm;

(c) emotional harm;

(d) economic harm;

(e) financial harm;

(f) serious harm to reputation; and

(g) other forms of serious harm that a reasonable person would identify as a possible outcome of the data breach.

Though individuals may be distressed or otherwise upset at an unauthorised access to or unauthorised disclosure or loss of their personal information, this is not in itself sufficient to require notification unless a reasonable person in the approved provider's position would consider that the likely consequences for those individuals would be serious harm.

5.3 Reasonable person test

In determining whether a reasonable person would consider that a data breach would be likely to result in serious harm we will have regard to the following factors:

(a) the kind of information;

(b) the sensitivity of the information;

(c) whether the information is protected by one or more security measures;

(d) if the information is protected by one or more security measures—the likelihood that any of those security measures could be overcome;

(e) the persons, or the kinds of persons, who have obtained, or who could obtain, the information;

(f) if a security technology or methodology;

(i) was used in relation to the information or methodology; and

(ii) was designed to make the information unintelligible or meaningless to persons who are not authorised to obtain the information.

6 Data breach response plan

6.1 We have implemented a *Data breach response plan* (Annexure 1) which sets out the steps we will follow if a data breach occurs.

6.2 The steps we will take as set out in our *Data breach response plan* (Annexure 1) include:

(a) Containing the breach and making a preliminary assessment;

(b) Evaluating the risks for individuals associated with the breach;

(c) Considering whether the data breach is an Eligible Data Breach and a breach notification is required;

(d) If notification is required, notifying:

(i) affected individuals; and

(ii) the OAIC;

(e) Considering whether others should be notified, for example:

(i) Police/law enforcement

(ii) professional or regulatory bodies

(iii) other agencies or organisations affected by the breach or those we are contractually required to notify;

(f) Reviewing the incident and taking action to prevent further breaches.

7 Notification

7.1 Notifiable data breach

In the event we have reasonable grounds to believe that an Eligible Data Breach has occurred, we are required to notify the OAIC and affected individuals as soon as practicable (unless an exception applies).

7.2 Notification to the Office of the Information Commissioner

In the event we are required to notify the Office of the Information Commissioner of an Eligible Data Breach, we may do so by using the *OAIC Notifiable Data Breach Statement* (Annexure 5), or such other method of notification that we consider appropriate in the circumstances.

7.3 Notification to affected individuals

In the event we are required to notify affected individuals of an Eligible Data Breach, we will do so by using the *Template notification letter to individuals at risk* (Annexure 4)

The notification to affected individuals will include:

(a) the organisation's (our) identity and contact details;

(b) a description of the data breach;

(c) the kinds of information concerned; and

(d) recommendations about the steps that individuals should take in response to the serious data breach.

7.4 Exceptions to notification

There are a number of exceptions to notification which may apply depending on the circumstances. These include:

(a) If compliance with the notification requirements would be inconsistent with another law of the Commonwealth that regulates the use or disclosure of information, we will be exempt to the extent of the inconsistency.

(b) If compliance would be inconsistent with another law of that kind which is prescribed in regulations under the Privacy Act, we will be exempt.

(c) If the notification requirements in the *My Health Records Act 2012* apply, then we are will be exempt to avoid double notification.

(d) If we have taken remedial action following an Eligible Data Breach or potential Eligible Data Breach and a reasonable person would conclude that:

(i) as a result of the remedial action, the unauthorised access or unauthorised disclosure of personal information (including an unauthorised access or unauthorised disclosure following loss of the information) is not likely to result in serious harm to the affected individuals; or

(ii) remedial action has prevented a loss of information from leading to an unauthorised access or disclosure,

then we will be exempt.

(e) If remedial action following an access or disclosure would lead a reasonable person to conclude that only particular individuals within a broader group are not likely to be at risk of serious harm following the remedial action, then we will not be required to notify those particular individuals (but would still be required to notify the remainder of the individuals).

(f) If the Commissioner has (at our request or at the Commissioner's own initiative) exempted us from providing notification of an Eligible Data Breach because the Commissioner is satisfied that it is reasonable in the circumstances to do so then we may be exempt altogether or for a period of time.

8 Media

8.1 All media inquiries must immediately be directed to the Administrator.

8.2 If a Worker receives an enquiry or request for information from a media representative the Worker must:

(a) decline to answer any questions;

(b) take the name, and contact details of the media representative making the inquiry;

(c) request that the person contact the Administrator; and

(d) advise the Administrator immediately of the inquiry.

8.3 No information is to be provided by any Worker to the media, even if it is ‘off the record’.

8.4 A short file note should be prepared by the Worker summarising the nature of any media inquiry and the information provided in response to any media inquiry and given to the Administrator.

9 Disciplinary action

Staff who fail to comply with this Data breach response policy may face disciplinary action and, in serious cases, termination of employment.

10 Documentation

10.1 To support and implement this policy and procedure we refer to related documentation including:

(a) Privacy Policy;

(b) Data breach response plan;

(c) Data breach matrix;

(d) Data breach incident report form;

(e) Template notification letter to individuals at risk;

(f) Template notification to the Office of the Information Commissioner.

Annexure 1 – Data breach response plan

This Data breach response plan sets out the procedure to be followed in the event a data breach occurs or a data breach is suspected to have occurred.

1 Identify

1.1 If a Worker becomes aware or starts to suspect that a data breach may have occurred, they must immediately notify the Privacy Officer.

1.2 If the Privacy Officer is notified or otherwise becomes aware of an actual or suspected data breach the Privacy Officer must:

(a) take immediate steps to contain the breach;

(b) commence a preliminary assessment of the breach;

(c) complete Part 1 of the *Data breach incident report form* (Annexure 3) in full including:

(i) Privacy Officer's details;

(ii) details of the person who reported the breach;

(iii) the date and time the data breach was discovered/notified;

(iv) the type of information which was involved in the breach;

(v) the cause and extent of the breach; and

(vi) details of any persons immediately notified of the breach;

(vii) details of any immediate action taken to contain the breach.

(d) report the breach to the Director of Care.

1.3 If the Privacy Officer is notified or otherwise becomes aware of an actual or suspected data breach, the Director of Care must:

(a) complete the *Data breach matrix* (Annexure 2);

(b) complete Part 2 of the *Data breach incident report form* (Annexure 3);

(c) follow the steps below, including to:

(i) assess the breach;

(ii) evaluate the breach;

(iii) determine whether the breach is notifiable;

(iv) if the breach is notifiable, notify the relevant parties;

(v) take action to prevent the same or similar breach occurring in the future;

(d) report the breach to the Administrator.

2 Contain

2.1 Once a data breach has been identified, immediate action must be taken by the manager on duty to contain the breach and mitigate any harm an individual or organisation may suffer as a result of the breach.

2.2 Where possible the Privacy Officer should consider taking the following immediate options:

(a) stop the unauthorised access;

(b) disable account or system access;

(c) engage appropriate IT services to recover the records;

(d) shut down the system which was subjected to the breach; and/or

(e) if it is not practical to shut down the system, consider revoking or changing computer access privileges or address weaknesses in the security.

3 Assess

3.1 The Director of Care is responsible for undertaking a preliminary assessment of the data breach and should consider the following questions while conducting the assessment:

(a) What information does the breach involve?

(b) What was the cause of the breach?

(c) What is the extent of the breach?

(d) What damage or harm has been or could be caused by the breach?

(e) How can the breach be contained?

3.2 If, when assessing the breach, the Director of Care forms a preliminary view that:

(a) the breach is not likely to result in serious harm, the Director of Care must:

(i) consider whether any action could be taken to prevent future breaches or potential breaches in accordance with section 6 below;

(ii) report to the Administrator and seek authorisation in writing for no further action to be taken;

(iii) record this decision, including reasons, using the *Data breach matrix* (Annexure 2) and *Data breach incident report form* (Annexure 3);

(b) the data breach or suspected data breach may result in serious harm to an individual or an organisation, the Director of Care must:

(i) inform the Administrator;

(ii) proceed with the steps below;

(iii) continue to take action where possible to contain the breach while carrying out the following steps.

4 Evaluate

4.1 If the Director of Care considers that the breach may result in serious harm, the Director of Care must follow the process outlined below.

4.2 Each breach needs to be evaluated on a case by case basis taking into account all of the relevant circumstances and assessing the risks involved.

4.3 In order to evaluate the risks associated with the data breach, the Director of Care should consider the following questions:

(a) The type of personal information involved;

(i) Does the type of personal information that has been compromised create a greater risk of harm?

(ii) Who is affected by the breach?

(b) The context of the affected information and the breach;

(i) What is the context of the personal information involved?

(ii) What parties have gained unauthorised access to the affected information?

(iii) Have there been other breaches that could have a cumulative effect?

(iv) How could the personal information be used?

(c) The cause and extent of the breach;

(i) Is there a risk of ongoing breaches or further exposure of the information?

(ii) Is there evidence of theft?

(iii) Is the personal information adequately encrypted, anonymised or otherwise not easily accessible?

(iv) What was the source of the breach?

(v) Has the personal information been recovered?

(vi) What steps have already been taken to mitigate the harm?

(vii) Is this a systemic problem or an isolated incident?

(viii) How many individuals are affected by the breach?

(d) The risk of serious harm to the affected individuals;

(i) Who is the recipient of the information?

(ii) What harm to individuals could result from the breach?

4.4 The Director of Care should also consider the broader implications of potential damage or harm caused to the organisation such as:

(a) loss of public faith and trust in the organisation;

(b) damage to reputation;

(c) civil or criminal liability;

(d) breach of any other privacy provisions or relevant laws.

4.5 Based on evaluation of the risks and factors set out above, the Director of Care in consultation with the Administrator must decide whether a reasonable person in the position of the approved provider would consider that the data breach would be likely to result in serious harm to the person/s to whom the information relates.

4.6 The Director of Care must document the decision and reasons using the *Data breach matrix* (Annexure 2) and *Data breach incident report form* (Annexure 3).

4.7 If the Director of Care decides:

(a) the breach is not likely to result in serious harm, Director of Care must:

(i) consider whether any action could be taken to prevent future breaches or potential breaches in accordance with section 6 below;

(ii) report to the Administrator and seek authorisation in writing for no further action to be taken;

(iii) record this decision, including reasons, using the *Data breach matrix* (Annexure 2) and *Data breach incident report form* (Annexure 3);

(b) the data breach or suspected data breach may result in serious harm to an individual or an organisation, the Director of Care must:

(i) inform the Administrator;

(ii) proceed with the steps below;

(iii) continue to take action where possible to contain the breach while carrying out the following steps.

5 Notification

5.1 Determine whether to notify

Based on evaluation of the risks and factors set out above, the Director of Care in consultation with the Administrator must decide whether to notify the affected individuals or organisations who are the subject of the breach. Each incident needs to be considered on a case-by-case basis to determine whether breach notification is required.

5.2 Notification not required if an exception applies

(a) In considering whether to notify the affected individuals or organisations who are the subject of the breach, the Director of Care in consultation with the Administrator must determine whether any exceptions to notification apply based on the particular circumstances. This includes considering whether any of the following relevant exceptions apply:

(i) Compliance with the notification requirements would be inconsistent with another law which regulates the use or disclosure of information.

(ii) Compliance would be inconsistent with another law prescribed in the Privacy Act.

(iii) The *My Heath Records Act 2012 applies*.

(iv) If remedial action has been taken, a reasonable person would conclude that:

(A) as a result of the remedial action, the unauthorised access or unauthorised disclosure of personal information is not likely to result in serious harm to the affected individuals; or

(B) remedial action has prevented a loss of information from leading to an unauthorised access or disclosure.

(v) If remedial action following an access or disclosure would lead a reasonable person to conclude that only particular individuals within a broader group are not likely to be at serious harm following the remedial action.

(vi) If the Commissioner has provided an exemption from providing notification because the Commissioner is satisfied that it is reasonable in the circumstances to do so.

(b) If the Director of Care in consultation with the Administrator is satisfied that an exception applies, then the organisation will be exempt from notifying. The extent of the exemption will depend on the circumstances, for example:

(i) the extent of any inconsistencies with any other laws regulating the use or disclosure of information;

(ii) the extent that the information is not likely to result in serious harm to the affected individuals; and

(iii) the extent of the conditions of any exemption given by the Commissioner.

5.3 Process for notification to affected individuals or organisations

(a) When to notify

If, after assessing the breach, the Director of Care in consultation with the Administrator determines that the data breach creates a real risk of serious harm to a person or an organisation, the approved provider must:

(i) as soon as practicable notify the Office of the Information Commissioner using the template in Annexure 5 or such other form of communication as the Director of Care in consultation with the Administrator considers appropriate;

(ii) promptly notify affected individuals or organisations who are the subject of the breach using the Template letter in Annexure 4 or such other form of communication as the Director of Care in consultation with the Administrator considers appropriate;.

(b) How to notify

In most instances, notification to the affected parties should be direct – by phone, letter, email or in person.

However, in instances where direct notification could cause further harm, is not cost effective or the contact details for the affected party is unknown, indirect notification may be performed. Indirect notification includes publication on a website, in the media or posted notices.

Further, the notification itself should not be bundled with other material as this may affect the impact of the breach and cause unnecessary confusion. Rather, the notification should be provided on its own, with only the necessary and relevant supporting documentation (if applicable).

Notification to the OAIC should be in writing.

(c) Who should be notified

Usually, it is only necessary to notify the persons and/or organisations who are or are likely to be affected by the breach. However, in some cases, it will be appropriate for the Director of Care to notify an individual's guardian or authorised representative as well as, or instead of, the individual.

(d) Information to be included in the notification

The following details should be included in a notification:

(i) a description of the breach/incident;

(ii) type of personal information involved;

(iii) an account of the organisation's response to the breach;

(iv) assistance offered to affected parties;

(v) other information sources designed to assist in protecting against identity theft or interferences with privacy, such as https://oaic.gov.au;

(vi) the organisations contact details;

(vii) whether a regulator or other external contact has been notified of the breach;

(viii) the legal implications;

(ix) information on how people or organisations can lodge a complaint with the organisation; and

(x) information on how people or organisations can lodge a complaint with the OAIC; and

(xi) information on how people or organisations can lodge a complaint with the relevant state or territory privacy or information regulator.

5.4 Other notifications

Depending on the type of breach and seriousness of the breach, the Director of Care in consultation with the Administrator must consider whether it is necessary or appropriate to notify other third parties including:

(a) Police;

(b) Insurance providers;

(c) Credit card companies and financial institutions;

(d) Professional or other regulatory bodies;

(e) Other internal or external parties who have not already been notified.

6 Prevent

6.1 Once the Director of Care has completed the above steps, the Director of Care should consider whether there are any changes which can be made within the organisation to improve:

(a) policies and procedures,

(b) staff practices,

(c) this Plan,

with a view to mitigating risk of a future data breach.

6.2 If there are changes which should be made within the organisation, the Director of Care should prepare a prevention plan to suggest actions that are proportionate to the significance of the breach and whether it was a systemic or isolated breach.

6.3 The prevention plan may include:

(a) a security audit of both physical and technical security;

(b) a review of policies and procedures and any changes to reflect the lessons learned from the investigation and conducting regular reviews;

(c) a review of employee selection and training practices; and

(d) a review of service delivery partners.

The Director of Care may wish to include a requirement for an audit at the end of the prevention plan to ensure it is implemented efficiently.

Annexure 2 – Data breach matrix

Using the matrix

This Data breach matrix should be used as part of the process of assessing and evaluating a data breach as outlined in the Data breach response plan (Annexure 1).

DATA BREACH MATRIX					
Type of impact	**Lowest ← Severity → Highest**				
	Minor = 1	**Low = 2**	**Moderate = 3**	**Major = 4**	**Extreme = 5**
The nature and type of information the breach involves [*sensitive information refers to information which is of a commercial, personal or proprietary nature and which may, if disclosed, impact upon individuals or organisations*]	No sensitive information pertaining to individuals or organisations exposed	Sensitive information exposed in respect of individuals or organisations which has the potential to cause only minor distress to the parties	Sensitive information exposed in respect of individuals or organisations which has the potential to cause substantial short term distress to the parties	Sensitive information exposed in respect of individuals and organisations which has the potential to cause substantial short to long term distress to the parties	Sensitive information exposed in respect of individuals and/or organisations which has the potential to cause significant long term distress to multiple parties, broad public concern, media coverage, Parliamentary inquiry or Royal Commission
The cause of the breach	No risk of ongoing or repeat breaches	Negligible risk of ongoing or repeat breaches and steps taken to mitigate any future risk	Moderate risk of ongoing breaches and further exposure of information, source of breach identified and steps being taken to mitigate	High risk of ongoing breaches and further exposure of information, source of breach not confirmed and steps being taken to mitigate	High risk of ongoing breaches and exposure of further information, evidence of theft, information not adequately anonymised and source of breach unknown
The extent of the breach	Little to no risk of serious harm to an individual or organisation	Risk of serious harm to a single individual or a small group of identifiable individuals	Risk of serious harm to multiple individuals or an organisation	Risk of serious harm to multiple individuals and organisations	Risk of serious harm to entire database of individuals, organisations and others

The damage or harm that has been or could be caused by the breach	No damage or harm caused. No future damage or harm forecasted	Minor and localised damage or harm has been or could be caused by the breach	Significant short term damage or harm has been or could be caused by the breach	Significant long term damage or harm has been or could be caused by the breach	Significant and widespread short and long term damage or harm has been or could be caused by the breach
Difficulty of containing the breach	Breach contained	Little to no risk that the breach will not be contained	Work underway to contain the breach. Moderate to low risk that breach will not be contained in the short term	The breach will not be contained in the short term and work is underway to contain the breach	Significant difficulty in containing the breach. Likelihood of breach being contained in the short to medium term, slim.
Risk of loss of public faith and trust in the organisation	No risk of loss of public faith and trust in the organisation	Minimal impact to public faith and trust in the organisation	Moderate impact to public faith and trust in the organisation over the short term	Significant impact to public faith and trust in the organisation over the short to medium term	Significant long term impact to public faith and trust in the organisation. Potential or actual consequences for organisations activities
Damage to reputation of organisation	No risk to the reputation of the organisation	Minimal impact on the reputation of the organisation	Moderate short-term impact to the reputation of the organisation	Significant impact to the reputation of the organisation over the short to medium term	Significant long term impact to the reputation of the organisation. Potential or actual consequences for organisations activities
Economic and commercial impact of the breach on the organisation	No economic or commercial impact on the organisation	Minimal economic or commercial impact on the organisation	Moderate short-term economic and commercial impact on the organisation	Significant economic and commercial impact on the organisation over the short to medium term	Significant short and long term economic and commercial impact on the organisation
Potential for civil or criminal liability resulting from the breach	No risk of civil or criminal liability	Minimal risk of civil or criminal liability	Moderate risk of civil or criminal liability	Significant of civil or criminal liability	Very high risk of civil or criminal liability
Has the incident breached any other privacy provisions or relevant laws	No breach of any other privacy provisions or laws	Breach of other privacy provisions or laws – minimal impact	Breach of other privacy provisions or laws – moderate impact	Breach of other privacy provisions or laws – significant impact	Breach of other privacy provisions or laws – very high impact

Matrix score
Minor – 10 to 18 points
Low – 19 to 26 points
Moderate – 27 to 35 points
High – 36 to 44 points
Extreme – 45 to 50 points

Please complete the matrix score to determine the risk profile of the data breach. The matrix score and data breach incident report form should be used in combination to determine the appropriate response to the breach and should be provided to the Chief Executive Officer as soon as practicable.

Annexure 3 – Data breach incident report form

PART 1 – TO BE COMPLETED BY MANAGER WHO FIRST RECEIVED NOTICE OF DATA BREACH			
Details of Manager reporting the incident			
Full name		**Title**	
Contact number			
How did you find out about the data breach			
Name of person who notified you			
☐ Male ☐ Female ☐ Staff ☐ Visitor ☐ Contractor ☐ Volunteer ☐ Client ☐ Other……			
Date of breach		**Time of breach**	am/pm
Date you were notified		**Time you were notified**	am/pm
Location of data breach			
Initial details of data breach			
Details of data which has been accessed			
Details of the extent of the data breach			
Details of any persons immediately notified of data breach			
Date persons notified		**Time persons notified**	am/pm
Did the person who notified you of the breach give any other relevant information about the breach?			

Describe immediate action taken to contain the breach (if any)			
You must notify the Director of Care of the data breach			
Date Director of Care notified	____/_____/_____	**Time Director of Care notified**	am/pm

PART 2 – TO BE COMPLETED BY MANAGER WHO IS RESPONSIBLE FOR ASSESSING AND RESPONDING TO THE DATA BREACH			
Details of Manager responsible for assessing and responding to the data breach			
Full name		**Title**	
Contact number			
Assessment (Refer to Data Breach Response Plan)			
What information does the breach involve?			
What was the cause of the breach?			
What is the extent of the breach?			
What damage or harm has been or could be caused by the breach?			
How can the breach be contained, if it has not been already?			
Evaluation of risks associated with the breach			
Risk associated with the type of personal information involved			
Who is affected by the breach?			
Does the type of personal information that has been compromised create a greater risk of harm?			
The context of the affected information and the breach			
What is the context of the personal information involved?			
What parties have gained unauthorised access to the affected information?			
Have there been other breaches that could have a cumulative effect?			
How could the personal information be used?			
The cause and extent of the breach			
Is there a risk of ongoing breaches or further exposure of the information?			
Is there evidence of theft?			
Is the personal information adequately encrypted,			

anonymised or otherwise not easily accessible?	
What was the source of the breach?	
Has the personal information been recovered?	
What steps have already been taken to mitigate the harm?	
Is this a systematic problem or an isolated incident?	
How many individuals are affected by the breach?	
The risk of serious harm to the affected individuals	
Who is the recipient of the information?	
What harm to individuals could result from the breach?	
Do you consider the data breach is an *eligible data breach* (refer to Data breach policy and procedure and Data breach response plan)	Yes ❑ No ❑ **If yes, the affected parties must be notified**
Notifying affected parties	
The Director of Care in consultation with the Administrator must determine whether it is necessary to notify affected individuals **(refer to the Data Breach Response Policy as a guide)**	
Notification to affected individuals must include	
A description of the breach/incident	Yes ❑ No ❑
Type of personal information involved	Yes ❑ No ❑
An account of the organisation's response to the breach	Yes ❑ No ❑
Assistance offered to affected parties	Yes ❑ No ❑
Other information sources designed to assist in protecting against identity theft or interferences with privacy, such as www.oaic.gov.au;	Yes ❑ No ❑
The organisations contact details	Yes ❑ No ❑
Whether a regulator or other external contact has been notified of the breach	Yes ❑ No ❑
The legal implications	Yes ❑ No ❑
Information on how people or organisations can lodge a complaint with the organisation	Yes ❑ No ❑
Information on how people or organisations can lodge a complaint with the OAIC	Yes ❑ No ❑

Information on how people or organisations can lodge a complaint with the relevant state or territory privacy or information regulator	Yes ❑ No ❑

Notification to third parties	
The Service Manager in consultation with the CEO must determine whether it is necessary to notify any of the following **(refer to the Data Breach Response Policy as a guide)**	
Office of the Australian Information Commissioner	Yes ❑ No ❑
Police	Yes ❑ No ❑
Insurance Provider	Yes ❑ No ❑
Credit card companies and financial institutions	Yes ❑ No ❑
Professional or other regulatory bodies	Yes ❑ No ❑
Other internal or external parties who have not already been notified	Yes ❑ No ❑
Agencies that have a direct relationship with the information, the subject of the breach	Yes ❑ No ❑

Other risks	
Detail whether there are any broader implications of the data breach to the organisation	
Loss of public faith and trust in the organisation?	Yes ❑ No ❑ (if yes, please provide detail below)
Damage to reputation?	Yes ❑ No ❑ (if yes, please provide detail below)
Liability?	Yes ❑ No ❑ (if yes, please provide detail below)
Breach of any other privacy provisions?	Yes ❑ No ❑ (if yes, please provide detail below)

Record of decision not to notify affected individuals, the OAIC or third parties
IF the Director of Care in consultation with the Administrator determined that it is not necessary to notify affected individuals, the OAIC or third parties of an eligible data breach, the decision (including reasons and any relevant exception) must be recorded here and the Administrator must sign off on the decision **(refer to the Data Breach Response Policy as a guide)**

Detail of reasons for decision not to notify
Administrator sign off on decision not to notify
Name of Administrator (print): **.....** **Signature .....** **Date** **Time**
Review
Consider whether there are any changes which can be made within the organisation which will help prevent future data breaches.

Name of Director of Care completing this report (print): **.....** **Signature .....** **Date** **Time**

Annexure 4 – Template notification letter to individuals at risk

[To be placed on provider's letterhead]

[Date]

[Name of individual who the breached data relates]

[Address]

[SUBURB] [STATE] [POSTCODE]

Email: [Email if applicable]

Dear [Name]

NOTIFICATION OF DATA BREACH

[Between/On] [insert period of time/date of breach], [insert summary of the data breach/incident]. The data accessed [may have included/included] personal information relating to you such as [identify the type of information at risk]. [To our knowledge, the data accessed did not include any [any types of information that we not involved in the data breach]].

We have taken the following steps to contain and minimise any further risk of harm due to the incident:

- [insert steps taken]

We recommend that you take the following steps in response to this data breach:

- [insert recommended steps]

St Louis values your privacy and deeply regrets that this incident occurred. St Louis is conducting a thorough review of the incident to prevent any recurrence.

If you have any questions, please do not hesitate to contact us on 08 8332 0950 or at [email].

[Provider signoff]

Please note the following document has been obtained directly from the OAIC website and may be updated from time to time.

Notifiable Data Breach statement

This form is used to inform the Australian Information Commissioner of an 'eligible data breach' where required by the Privacy Act 1988.

Part one is the 'statement' about a data breach required by section 26WK of the Privacy Act.

If you are required to notify individuals of the breach, in your notification to those individuals you must provide them with the information you have entered into part one of the form.

The OAIC encourages entities to voluntarily provide additional information about the eligible data breach in part two of this form. Part two of the form is optional, but the OAIC may need to contact you to seek further information if you do not complete this part of the form.

Before completing this form, we recommend that you read our resource *What to include in an eligible data breach statement*.

If you are unsure whether your entity has experienced an eligible data breach, you may wish to review the *Identifying eligible data breaches* resource.

The OAIC will send an acknowledgement of your statement about an eligible data breach on receipt with a reference number.

Your personal information

We will handle personal information collected in this form (usually only your name and contact details) in accordance with the Australian Privacy Principles.

We collect this information to consider and respond to your breach notification. We may use it to contact you.

For more information about how the OAIC handles personal information is available in our privacy policy.

Part one — Statement about an eligible data breach

The information that you provide to the OAIC in part one of this form must also be included in your notification to individuals (if notification is required).

1. Organisation/agency details (You must complete this section)

Organisation/agency name:

Phone:

Email:

Address

Address Line 1:

Address Line 2:

Suburb:

State:

Postcode:

Other contact details:

2. Description of the eligible data breach (You must complete this section)**:**

3. Information involved in the data breach (You must complete this section):

Kind or kinds of personal information involved in the data breach

Please select all that apply:

- ☐ Financial details
- ☐ Government identifiers (e.g. Centrelink Reference Number, Medicare number)
- ☐ Tax File Number (TFN)
- ☐ Contact information (e.g. home address, phone number, email address)
- ☐ Health information
- ☐ Other sensitive information (such as sexual orientation, gender identity, political or religious views)
- ☐ Other (please specify):

4. Recommended steps (You must complete this section):

Steps your organisation/agency recommends that individuals take to reduce the risk that they experience serious harm as a result of this data breach:

5. Other entities affected (This section is optional):

If the data breach described above was also a data breach of another organisation/agency, you may provide their identity and contact details.

Was another organisation/agency affected?

☐ Yes

☐ No

If you answered yes, please provide contact details for the organisation/agency:

Organisation/agency name:

Phone:

Email address:

Address

Address Line 1:

Address Line 2:

Suburb:

State:

Postcode:

Other contact details:

Part two — Additional information

The OAIC encourages entities to provide additional information to assist us in understanding the eligible data breach. Part two of the form is optional, but the OAIC may need to contact you to seek further information if you do not complete this part of the form.

The information that you provide on part two of the form does not need to be included in your notification to individuals, and you may request that it be held in confidence by the OAIC.

1. Your contact details:

Title:

First name:

Last name:

Phone:

Email address:

2. Date the breach occurred (if known) (DD/MM/YYYY):

3. Date the breach was discovered (DD/MM/YYYY):

4. Primary cause of the data breach (choose only one):

- ☐ Malicious or criminal attack
- ☐ System fault
- ☐ Human error

5. Description of how the data breach occurred:

6. Number of individuals whose personal information is involved in the data breach (choose only one)

- ☐ 1
- ☐ 2 – 10
- ☐ 11 – 100
- ☐ 101 – 1,000
- ☐ 1,001 – 10,000
- ☐ 10,001 – 100,000
- ☐ 100,001 – 1,000,000
- ☐ 1,000,001 – 10,000,000
- ☐ 10,000,001 or more

7. Exact number of individuals whose personal information is involved in the data breach (you can provide your best estimate at this stage):

8. Description of any action you have taken to assist individuals whose personal information was involved in the data breach:

9. **Description of any action you have taken to prevent reoccurrence:**

10. **How do you intend to notify individuals who are likely to be at risk of serious harm as a result of the data breach? When will this occur?:**

11. **List any other data protection authorities, law enforcement bodies or regulatory bodies that you have reported this breach to:**

12. **Is there any other information you wish to provide at this stage, or any matters that you wish to draw to the OAIC's attention?:**

    You can provide additional information below, or attach supporting documents when you submit this form.

☐ I request that the information provided in part two of this form is held by the OAIC in confidence.

The OAIC will respect the confidence of commercially sensitive information provided voluntarily in support of a data breach notification, and will only disclose this information after consulting with you, and with your agreement or where required by law.

If you request the information in part two of this form is held by the OAIC in confidence, please provide further information to support the request: