Purpose of EMPHN's Data Breach Response Statement

This statement outlines how EMPHN manages data breaches; involving the unauthorised access, disclosure or loss of personal information – whether the cause is malicious, human error or system failure.

Drawing on our Privacy Policy and our Data Governance Framework, our process aligns with our legislative obligations according to the Office of the Australian Information Commissioner, the Australian Privacy Principles and the Privacy Amendment (Notifiable Data Breaches) (2017) within the Privacy Act 1988, the Commonwealth (2012) and Victorian (2001) Health Records Acts, and the Victorian Privacy and Data Protection Act 2014.

EMPHN's 4-step response plan

1. Raise the alert and contain the breach

When a data breach is suspected or has occurred, any staff member who becomes aware of this must immediately alert their direct manager, as well as the Data Steward who owns the given dataset, and the Privacy Officer, outlining:

- time and date the data breach occurred or was discovered
- type of personal information involved
- cause and extent of the breach – or if unknown, how the breach was identified
- systems affected
- what corrective action has been taken to contain the breach

2. Assess risk and potential impact for affected individuals

The Data Steward who owns the given dataset, and the Privacy Officer determine whether to escalate the data breach to the Data Breach Response Team, asking:

- Are multiple individuals affected by the breach or suspected breach?
- Is there potentially risk of serious harm to the affected individuals?
    - What type of personal information is involved? Is it sensitive information?
    - Was the breach malicious with intent to cause harm?
    - Are any effective protections in still place on the breached data? (e.g. is it encrypted, anonymised or otherwise not easily accessible)
    - What harm is the breach likely to cause to the owners of the personal information?
    - What has been done to remedy the breach and did they work?

For less serious incidents, the Privacy Officer completes an incident report in TICKIT, recording:

- remedial action taken
- outcome of the action taken
- mitigation strategies implemented to prevent recurrence

If the breach, or suspected breach, carries high risk or likelihood of significant impact for the affected individuals; indicates a systemic problem with EMPHN's processes or procedures; or could draw media or stakeholder attention, the Privacy Officer escalates to the Data Breach Response Team.

3. Notification and escalation

Each data breach is dealt with on a case-by-case basis, with the risk assessment determining what actions are to be taken. The Privacy Officer convenes the Response Team to:

Contain the breach

- Immediately contain the breach if this has not yet occurred, such as retrieving lost data, ceasing unauthorised access, shutting down, isolating affected systems, or consulting with other entities that jointly hold data with EMPHN.
- Inform the Executive and provide ongoing updates of key developments.
- Collect evidence to determine the cause or allow appropriate corrective action.
- Seek expertise with other staff or externally (such as cyber security or legal expertise) as appropriate.
- If appropriate, develop a communication strategy including content and method.

Evaluate the risks for individuals associated with the breach

- Conduct an initial investigation from the information collected about the breach.
- Establish the cause and extent of the breach.
- Assess priorities and risks based on what is known.
- Keep appropriate records of the suspected breach and actions of the Response Team, including the steps taken to rectify the situation and the decisions made.

Activate breach notification

- Determine who needs to be made aware of the breach (internally such as the Board Chair and potentially externally).
- Notify affected individuals and OAIC if the data breach creates a real risk of serious harm to an individual and remedial action cannot prevent the likely risk of serious harm.
    - The Communications and Engagement Manager is to notify the affected individuals by phone, letter, email, or in person).
    - Indirect notification (e.g. by website or media) should only be used where direct notification could cause further harm, is cost prohibitive or the contact information of affected individuals is unknown.
- The Privacy Officer completes the Notifiable Data Breach form on the OAIC's website.

Incidents involving another entity

If the data breach involves another entity that jointly holds Personal Information with EMPHN, for example an entity that has physical possession of the information, the Privacy Officer leads discussions with the other entity to determine responsibilities under the Notifiable Data Breach Scheme.

Only one entity is required to assess the breach, and only one entity is required to notify the OAIC and affected individuals. The entity with the most direct relationship with the individual/s affected by the data breach should carry out the notification.

4. Take action to prevent future breaches

The Data Breach Response Team must submit a report to the Information Management and Data Governance (IMDG) Steering Committee on outcomes and recommendations:

- Root cause analysis of the data breach
- Actions taken, including remedial action and notification of the data breach
- Risk mitigation strategies to reduce the likelihood of recurrence
- Recommendations for changes to related policies and procedures to reflect lessons learned
- Relevant updates made to the Policy Directory and schedule to ensure changes are made during next review

Where to find out more about EMPHN's data breach response

- **For general enquiries, contact: policies@emphn.org.au**
- For enquires about this statement, contact: **Executive Director Strategy and Service Design**
- You can also provide feedback on this statement, or EMPHN's handling of a breach via our feedback facility on our website.
- If you contact EMPHN and have not been responded to satisfactorily after 30 days, you can file a written complaint with the Office of the Australian Information Commissioner (OAIC) or the Commonwealth Department of Health within 12 months of when you believe your personal information was breached.