

# **Data Breach Response Statement**

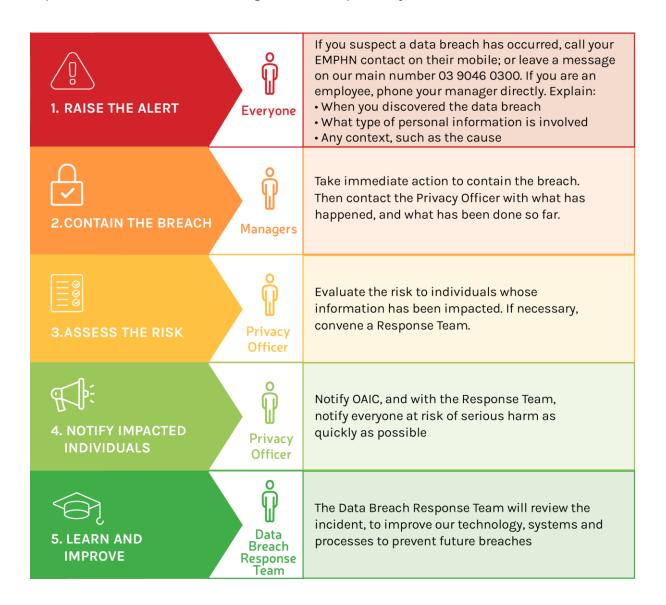
### **Purpose**

This Data Breach Response Statement defines how EMPHN responds to data breaches.

A data breach refers to the loss, unauthorised access or disclosure of commercial, confidential or personal information held by EMPHN; whether as a result of malicious action, human error or system failure.

Our process is designed to contain, assess and respond to data breaches quickly; and to prevent or minimise harm to individuals who are impacted by the data breach. It also ensures we comply with relevant legislation, and the Office of the Australian Information Commissioner's (OAIC) Notifiable Data Breaches Scheme. Responding to a data breach

The steps in EMPHN's 5-step Data Breach Response Plan are typically rolled out simultaneously or in quick succession. At all times, responsible officers must ascertain what can be done to reduce actual or potential harm to individuals or organisations impacted by the data breach.



#### **Data Breach Response Statement**



## Most importantly

If a breach impacts your personal information, potentially causing serious harm to you, we will notify you. We will also explain what we are doing to remedy the breach.

#### Where to find out more

- For enquires about this Statement, contact EMPHN's Privacy Officer: privacyofficer@emphn.org.au
- You can provide feedback on EMPHN's handling of a breach via the feedback facility on our website.
- If you contact EMPHN and after 30 days you believe our response is unsatisfactory, you can
  file a written complaint with the Office of the Australian Information Commissioner (OAIC) or
  the Commonwealth Department of Health. You must do this within 12 months of when you
  believe your personal information was breached.