DATA BREACH RESPONSE PLAN

VERSION	1.0
DOCUMENT AUTHOR	Data Governance Committee
APPROVED BY	EIS Health Ltd. Board
EFFECTIVE DATE	31 March 2020

EIS Health Ltd.

Contents

Overview

CESPHN is committed to managing Personal Information it holds in compliance with the *Privacy Act 1988 (Cth)* (Privacy Act) and the *Health Records and Information Privacy Act 2002 (NSW)* (HRIP Act). The Data Breach Response Plan (Plan) forms part of CESPHN's Privacy Policy and Procedure.

Under the Notifiable Data Breaches Scheme any organisation or agency covered by the *Privacy Act* must notify the Office of Australian Information Commissioner (OAIC) and affected individuals when a data breach is likely to result in Serious Harm to an individual whose Personal Information is involved.

This data breach response plan outlines definitions, sets out procedures and clear lines of responsibility for staff in the event that CESPHN experiences a data breach or suspects that a data breach has occurred. The response plan is intended to enable CESPHN to contain, assess and respond to data breaches in a timely fashion and to help mitigate Serious Harm to affected individuals.

EIS reserves the right to amend, supplement, replace or rescind any part of this procedure as it deems appropriate in its sole and absolute discretion from time to time.

Definitions

Data Breach	Loss, Unauthorised Access or Unauthorised Disclosure of Personal Information
Data Custodian	Person delegated by the data sponsor who is responsible for the day to day oversight of a data asset including the location of data and metadata, approval of access to data and the overall quality and security of the data
Notifiable Data Breach	A Notifiable Data Breach occurs when the following three criteria are satisfied: ▪ There is loss, Unauthorised Access or Unauthorised Disclosure of Personal Information held ▪ The loss, access, or disclosure is likely to result in serious harm to any of the individuals to whom the information relates ▪ Remedial action is not able to prevent the likely risk of serious harm.
Personal Information	Has the same meaning as in the Privacy Act: information or opinion about an identified individual, or an individual who is reasonably identifiable whether the information or opinion is true or not; and whether the information or opinion is recorded in a material form or not. This can include sensitive and health information.
Unauthorised Access	Occurs when Personal Information held is accessed by someone who is not permitted to have access. This can include unauthorised access by an employee, a contractor or an external third party (such as by hacking)
Unauthorised Disclosure	Occurs when an entity, whether intentionally or unintentionally, makes Personal Information accessible or visible to others outside the entity and releases that information from its effective control in a way that is not permitted by the Privacy Act.

Data Breach Response Team

Response Team Membership

Role	Responsibility
Privacy Officer	Leading the response team, reporting to the Executive Management Team, and (if deemed necessary) notifying the OAIC
Data Custodian	Custodian of data affected by the data breach
Marketing and Communications Manager	Developing the communications strategy and notifying affected individuals and media (if deemed necessary)
Systems Administrator	Supporting root cause analysis and impact of data breach that involves ICT systems
Data Governance Secretariat	Response Team coordinator

Data breach response process

If any CESPHN staff member suspects or becomes aware of a data breach, this plan must be activated and followed.

1. Alert your manager, relevant Data Custodian and Privacy Officer

When a data breach is suspected or has occurred, any staff member who becomes aware of this must immediately alert their manager, the relevant Data Custodian, and the Privacy Officer and, using the Data Breach Notification Form in Folio, advise them:

- Time and date the data breach occurred/ was discovered
- Type of Personal Information involved
- Cause and extent of the breach or if unknown, how the breach was identified
- Systems affected
- Any corrective action that has occurred to contain the breach.

2. Assess risk and potential impact for affected individuals

The manager, Data Custodian and Privacy Officer must determine whether to escalate the data breach to the Response Team by considering the following:

- Are multiple individuals affected by the breach or suspected breach?
- Is there, or could there be, a real risk of serious harm to the affected individuals?
    - What type of Personal Information is involved (and in particular, is it sensitive information)?
    - Who are the recipients of the Personal Information and what is the likelihood that they would want to cause harm to the individuals to whom the information relates?
    - Are there any protections that would prevent the party who receives (or may have received) the Personal Information from using it (e.g. is it encrypted, anonymised or otherwise not easily accessible) and what is the likelihood that any of these protections could be overcome?
    - What is the nature of the harm that could arise from the breach (e.g. is the individual likely to suffer identity theft, financial loss, threats to physical safety, loss of business or employment opportunities, workplace or social bullying or marginalisation, humiliation, embarrassment, damage to reputation or relationships)?
    - What steps have been taken to remedy the breach (and how certain are we that they are effective)?

- Does the breach or suspected breach indicate a systemic problem to CESPHN's processes or procedures?
- Could there be media or stakeholder attention as a result of the actual or suspected breach?

If the answer to any of these questions is 'yes' then the Privacy Officer is to escalate the data breach to the Response Team (see **Step 3**). In all other instances, the Privacy Officer is to complete the Data Breach Notification Form including responses to the following questions:

- Remedial action taken
- Outcome of the action taken
- Mitigation strategies implemented to prevent recurrence
- Recommendation that no further action is required.

The Response Team Coordinator is to provide the documentation to the Executive Management Team and Data Governance Committee for noting.

3. Escalation to Response Team

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

3.1 Contain the breach

- Immediately contain the breach if this has not yet occurred. This may include retrieval of lost data, ceasing Unauthorised Access, shutting down, isolating affected systems, or consulting with other entities that jointly hold data with CESPHN.
- Inform the Executive Management Team and provide ongoing updates of key developments.
- Collect all evidence of the breach to determine the cause of the breach 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.

3.2 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.

3.3 Consider 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 the OAIC if the data breach creates a real risk of serious harm to an individual (see assessment under Step 2) and remedial action is not able to prevent the likely risk of serious harm:
    - The Marketing and Communications Manager is to notify the affected individuals. Notification should be direct (e.g. 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 is to complete the Notifiable Data Breach form on the OAIC's website.

3.4 Take action to prevent future breaches

- Submit a report to the Data Governance Committee and Executive Management Team 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.

Documents created by the Response Team should be saved in the Data Governance Committee folder and attached to the Data Breach Notification Form in Folio.

Incidents involving another entity

If the data breach involves another entity that jointly holds Personal Information with CESPHN, for example an entity that has physical possession of the information, the Privacy Officer will lead 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.

NSW Government Agencies

Under the *Data Sharing (Government Sector) Act 2015 (NSW),* if the data breach involves personal or health information shared by a NSW government agency, CESPHN must also inform the data provider and the NSW Privacy Commissioner (IPC) of the breach. Notification of data breaches to the IPC must be submitted by the Privacy Officer using the IPC Data Breach Form.

Contacts

For any queries regarding this policy, please contact the Privacy Officer (General Manager of Corporate Services).

Procedure document control

Documents related to this policy
Data Governance Framework
Privacy Policy and Procedure
Cyber Security Policy and Procedure
IT Infrastructure Policy and Procedure
Data Sharing and Release Procedure
Risk Management Policy
Risk Management Procedure