Nangganawili Aboriginal Community Controlled
Health and Medical Services Aboriginal Corporation

ICN 1870 ABN 85 650 098 620

44 Scotia Street, Wiluna WA 6646
PO Box 40, Wiluna WA 6646
Telephone (08) 9981 8600
Fax: (08) 9981 8660
info@nahs.org.au
www.nahs.org.au

Mandatory Data Breach Response Policy

1. Policy & Rationale

The purpose of this policy is to guide staff in the mandatory procedures that must be applied in the event Nangganawili Aboriginal Health Service experiences a data breach or suspects that a data breach has occurred.

This policy in conjunction with the Data Breach Incident Report Form is intended to enable Nangganawili Aboriginal Health Service to contain, assess and respond to data breaches in a timely fashion, to help mitigate potential harm to affected individuals.

The Privacy Act 1988 (Cth) has been amended by the *Privacy Amendment (Notifiable Data Breaches) Act 2017*, which establishes a Notifiable Data Breaches (NDB) Scheme in Australia. The NDB scheme requires organisations covered by the *Australian Privacy Act 1988 (Privacy Act)* to notify any individuals likely to be at risk of serious harm by a data breach.

The NDB scheme commenced on the 22nd of February 2018 and only applies to eligible data breaches that occur on, or after, that date. Data breaches discovered before 22nd February 2018 are not subject to the scheme. If the health service discovers a breach after 22nd February 2018, but the breach occurred prior to that date, the breach is not an eligible data breach for the purposes of the NDB scheme.

Not all data breaches are notifiable. The NDB scheme only requires the organisation to notify when there is a data breach that is likely to result in serious harm to any individual to whom the information relates.

If the health service is required to take a reasonable and expeditious assessment to determine if the data breach is likely to result in serious harm. The health service must take reasonable steps to complete the assessment of the suspected data breach within 30 days.

If the health service has reasonable grounds to believe that there has been a notifiable data breach, then it must provide a statement to the Australian Information Commissioner which sets out matters including:

- the identity and contact details of the organisation
- a description of the data breach
- the kinds of information concerned and;
- recommendations about the steps individuals should take in response to the data breach.

As soon as practicable after preparing the statement for the Australian Information Commissioner, the health service must also take reasonable steps to notify the statement information to either

44 Scotia Street, Wiluna WA 6646
PO Box 40, Wiluna WA 6646
Telephone (08) 9981 8600
Fax: (08) 9981 8660
info@nahs.org.au
www.nahs.org.au

each individual to whom the information relates; or if not all individuals are deemed to be 'at risk of serious harm', only those affected individuals who are deemed 'at risk'.

Failure to adhere to this policy may result in:

- Failure to meet obligations under the Privacy Act resulting in civil penalties
- Adverse media or stakeholder attention
- Erosion of public confidence in the health service's capacity to protect personal information by properly responding to a data breach

2. Definitions

Notificable Data Breach: is a data breach that is likely to result in serious harm to any of the individuals to whom the information relates.

Serious Harm: could include: serious physical, psychological, emotional, economic and financial harm, as well as serious harm to reputation and other forms of serious harm that a reasonable person in the health service's position would identify as a possible outcome of the data breach.

Data Breach: A data breach occurs when personal information is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference. Examples of a data breach include when:

- a device containing patient information is lost or stolen
- the health service's database containing personal information is hacked
- personal information is mistakenly provided to the wrong person.

Personal Information: The Privacy Act defines personal information as 'information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable'. Common examples are an individual's name, signature, address, telephone number, date of birth, medical records, bank account details and commentary or opinion about a person.

3. Procedure

When a data breach is discovered by a NAHS staff member or NAHS is otherwise alerted to a data breach or suspected data breach, a Data Breach Incident Report Form is to be completed. The form is to be completed immediately by the person who discovers or suspects the breach. The following details must be recorded:

- the date, time, duration and location of the breach
- how the breach was discovered or is suspected
- description of the incident and the type of data involved in the breach

Nganggananawili Aboriginal Community Controlled
Health and Medical Services Aboriginal Corporation
ICN 1870 ABN 85 650 098 620

44 Scotia Street, Wiluna WA 6646
PO Box 40, Wiluna WA 6646
Telephone (08) 9981 8600
Fax: (08) 9981 8660
info@nahs.org.au
www.nahs.org.au

- the cause and extent of the breach
- other staff members that either witnessed the event or were notified at the time of the incident

Once completed the Data Breach Incident Report Form is to be forwarded to the Policy & Compliance Manager who will form a Data Breach Response Team.

There are four key steps to consider when responding to a breach or suspected breach:

Step 1: Contain the breach and make a preliminary assessment

- The health service's first step is to contain a suspected or known breach where possible. This means taking immediate steps to limit any further access or distribution of the affected personal information, or the possible compromise of other information.

Step 2: Evaluate the risks for individuals associated with the breach

- Consider whether the data breach is likely to result in serious harm to any of the individuals whose information was involved. If the health service has reasonable grounds to believe this is the case, then it must notify the individuals affected and the Information Commissioner. If there is only grounds to suspect that this is the case, then conduct an assessment process. As part of the assessment, consider whether remedial action is possible.
- The assessment is conducted in three stages:
    - **Initiate:** plan the assessment and assign a team or person
    - **Investigate:** gather relevant information about the incident to determine what has occurred
    - **Evaluate:** make and document an evidence-based decision about whether serious harm is likely.
- The assessment should be conducted expeditiously and, where possible, within 30 days. If it cannot be done within 30 days, document why this is the case.
- Where possible, take steps to reduce any potential harm to individuals. This might involve taking action to recover lost information before it is accessed, or changing access controls on compromised programs before unauthorised access occurs.
- If remedial action is successful in making serious harm no longer likely, then notification is not required and the health service can progress to the 'review' stage.

Nganggananawili Aboriginal Community Controlled
Health and Medical Services Aboriginal Corporation
ICN 1870 ABN 85 650 098 620

44 Scotia Street, Wiluna WA 6646
PO Box 40, Wiluna WA 6646
Telephone (08) 9981 8600
Fax: (08) 9981 8660
info@nahs.org.au
www.nahs.org.au

Step 3: Consider breach notification

- Where remedial action is not successful and serious harm is likely, the health service must prepare a statement for the Commissioner that contains:
    - the health service's identity and contact details
    - a description of the breach
    - the kind/s of information concerned
    - recommended steps for individuals
- The health service must also notify affected individuals, and inform them of the contents of the statement made to the Commissioner. There are three options for notifying:
    - Option 1: Notify all individuals
    - Option 2: Notify only those individuals at risk of serious harm

  If neither of these options are practicable:
    - Option 3: Publish the statement on the health service's website and publicise it

Step 4: Review the incident and take action to prevent future breaches

- Review the incident and take action to prevent future breaches.
    - Fully investigate the cause of the breach
    - Develop a prevention plan
    - Conduct audits to ensure the plan is implemented
    - Update security/response plan
    - Consider changes to policies and procedures
    - Revise staff training
- Also consider reporting the incident to other relevant bodies, such as:
    - police or law enforcement
    - ASIC, APRA or the ATO

44 Scotia Street, Wiluna WA 6646
PO Box 40, Wiluna WA 6646
Telephone (08) 9981 8600
Fax: (08) 9981 8660
info@nahs.org.au
www.nahs.org.au

- The Australian Cyber Security Centre
- Professional bodies
- Financial services provider

4. Responsibilities

This policy applies to all persons employed or engaged by Nganggananawili Aboriginal Health Service (including contractors, students, volunteers and agency personnel), and the scope of the policy includes NAHS data held in any format or medium (paper-based or electronic) that contains personal information.

The policy should be reviewed every 3 years, or sooner if required, by the Policy & Compliance Manager.

5. Evidence Base

- Privacy Amendment (Notifiable Data Breaches) Act 2017
- Australian Government Officer of the Australian Information Commissioner, Data Breach Response Plan
- Australian Government Officer of the Australian Information Commissioner, Guide to Developing a Data Breach Response Plan, April 2016
- Government of WA Department of Health, Data Breach Response Policy, September 2014

6. Related Documents

- Doc_421 Data Breach Incident Report Form V1