Suite 2, 2A Cowper St
Parramatta NSW 2150

Phone: 02 9891 2255
Fax: 02 9806 9731
Email: info@heartbeatnursing.com.au
www.heartbeatnursing.com.au

ABN: 49 084 686 760

Data Breach Policy and Response Plan

Aim:

This Policy sets out the processes to be followed by Heartbeat Nursing Agency Pty Ltd staff in the event that Heartbeat Nursing Agency experiences a data breach or suspects that a data breach has occurred. A data breach involves the loss of, unauthorised access to, or unauthorised disclosure of, personal information.

Scope:

This policy is relevant to all staff employed by Heartbeat Nursing Agency Pty Ltd.

Procedure:

Heartbeat Nursing Agency Pty Ltd is committed to managing personal information in accordance with the Privacy Act 1988 (incorporating the Australian Privacy Principles). This document should be read in conjunction with the Privacy Policy.

A data breach involves the loss of, unauthorised access to, or unauthorised disclosure of, personal information.

The Privacy Amendment (Notifiable Data Breaches) Act 2017 (NDB Act) established a Notifiable Data Breaches (NDB) scheme requiring organisations covered by the Act to notify any individuals likely to be at risk of *serious harm* by a data breach.

The Office of the Australian Information Commissioner (OAIC) must also be notified.

Accordingly, Heartbeat Nursing Agency Pty Ltd needs to be prepared to act quickly in the event of a data breach (or suspected breach), and determine whether it is likely to result in serious harm and whether it constitutes an Notifiable Data Breach.

Adherence to this Procedure and Response Plan will ensure that Heartbeat Nursing Agency Pty Ltd can contain, assess and respond to data breaches expeditiously and mitigate potential harm to the person(s) affected.

This Procedure and Response Plan has been informed by:

- The Office of the Australian Information Commissioner's "Guide to developing a data breach response plan"
- The Office of the Australian Information Commissioner's "Data breach notification guide: a guide to handling personal information security breaches"
- NDB Act
- The Act and Australian Privacy Principles (Schedule 1 of the Act)

Suite 2, 2A Cowper St
Parramatta NSW 2150

Phone: 02 9891 2255
Fax: 02 9806 9731
Email: info@heartbeatnursing.com.au
www.heartbeatnursing.com.au

ABN: 49 084 686 760

Procedure to follow where a data breach occurs or is suspected

1. **Alert**

Where a privacy data breach is known to have occurred (or is suspected) by a person who becomes aware of this must alert the Heartbeat Nursing Agency's Operations Manager or the Managing Director. Via a telephone call or email.

The Information that should be provided (if known) at this point includes:

a) When the breach occurred (time and date)

b) Description of the breach (type of personal information involved)

c) Cause of the breach (if known) otherwise how it was discovered

d) Which system(s) if any are affected?

e) Whether corrective action has occurred to remedy or ameliorate the breach (or suspected breach)

2. **Assess and determine the potential impact**

Once notified of the information above, the Operations Manager or the Managing Director must consider whether a privacy data breach has (or is likely to have) occurred and make a preliminary judgement as to its severity.

The IT Service Provider and Insurers will be contacted for advice.

3. **Criteria for determining whether a privacy data breach has occurred**

a) Is personal information involved?

b) Is the personal information of a sensitive nature?

c) Has there been unauthorised access to personal information, or unauthorised disclosure of personal information, or loss of personal information in circumstances where access to the information is likely to occur?

4. **Criteria for determining severity**

a) The type and extent of personal information involved

b) Whether multiple individuals have been affected

c) Whether the information is protected by any security measures (password protection or encryption)

d) The person or kinds of people who now have access

e) Whether there is (or could there be) a real risk of serious harm to the affected individuals

Suite 2, 2A Cowper St
Parramatta NSW 2150

Phone: 02 9891 2255
Fax: 02 9806 9731
Email: info@heartbeatnursing.com.au
www.heartbeatnursing.com.au

ABN: 49 084 686 760

f) Whether there could be media or stakeholder attention as a result of the breach or suspect breach

Serious harm could include physical, physiological, emotional, and economic/financial or harm to reputation and is defined in section 26WG of the NDB Act.

Having considered the matters above in consultation with the IT Service providers, the Operations Manager or the Managing Director will determine whether the data breach should be escalated to the Data Breach Response Team. This will depend on the nature and severity of the breach.

Data breach managed at the Hospital/Consulting room level

Where the Operations Manager or the Managing Director instructs that the data breach is to be managed at the local level, the Operations Manager or the Managing Director or relevant Manager must:

- ensure that immediate corrective action is taken, if this has not already occurred (corrective action may include: retrieval or recovery of the personal information, ceasing unauthorised access, shutting down or isolating the affected system); and
- submit an incident report

The incident report must contain the following:

- Description of breach or suspected breach
- Action taken
- Outcome of action
- Processes that have been implemented to prevent a repeat of the situation.

Data breach managed by the Response Team

Where the Operations Manager or IT Service Provider determines that the data breach must be escalated to the Response team, the Operations Manager will convene the IT Team and notify the Managing Director.

The Response team will consist of:

- IT Supplier – Team leader/ Operations Manager - Response coordinator
- IT Service Provider - IT support/forensics support and to assist in reviewing security and monitoring controls related to the breach (for example, access, authentication, encryption, audit logs) and to provide advice on recording the response to the data breach
- Operations Manager – May be asked to assist with corrective action and notification of persons affected by the breach
- Lawyer – As applicable to identify legal obligations and provide advice
- Insurers – To provide advice and support

Suite 2, 2A Cowper St
Parramatta NSW 2150

Phone: 02 9891 2255
Fax: 02 9806 9731
Email: info@heartbeatnursing.com.au
www.heartbeatnursing.com.au

ABN: 49 084 686 760

- Media/communications expert may be utilised to assist in communicating with affected individuals and dealing with the media and external stakeholders.

Role of the Response Team

There is no single method of responding to a data breach and each incident must be dealt with on a case by case basis by assessing the circumstances and associated risks to inform the appropriate course of action.

The following steps may be undertaken by the Response Team (as appropriate):

- Immediately contain the breach (if this has not already occurred). Corrective action may include: retrieval or recovery of the personal information, ceasing unauthorised access, shutting down or isolating the affected system.
- evaluate the risks associated with the breach, including collecting and documenting all available evidence of the breach
- Call upon the expertise the IT Service Provider
- Notify Insurers (Lawyers as applicable)
- Engage an independent cyber security or forensic expert if indicated
- Assess whether serious harm is likely (with reference to section 26WG of the NDB Act)
- Determine whether this breach constitutes an NDB for the purpose of mandatory reporting to the OAIC, Sydney NSW (TEL 1300 363 992) and the practicality of notifying affected individuals.
- Consider developing a communication or media strategy including the timing, content and method of any announcements to, staff, patients or the media.
- Take steps to prevent a further occurrence

The Response Team must undertake its assessment within 48 hours of being convened.

Notification

If it is determined that the breach meets the criteria as a Notifiable Breach, the Managing Director must prepare a prescribed statement and provide a copy to the OAIC and NSW State Regulatory Body as soon as practicable (and no later than 30 days after becoming aware of the breach or suspected breach).

Managing Director must also notify each individual to whom the relevant personal information relates. Where impracticable the Managing Director must take reasonable steps to publicise the statement.

Suite 2, 2A Cowper St
Parramatta NSW 2150

Phone: 02 9891 2255
Fax: 02 9806 9731
Email: info@heartbeatnursing.com.au
www.heartbeatnursing.com.au

ABN: 49 084 686 760

Information required in Notification Statement to OAIC/ NSW **State Regulatory Body**

Supporting documents/Documents of interest

Heartbeat Privacy Policy

The Office of the Australian Information Commissioner's "Guide to developing a data breach response plan"

The Office of the Australian Information Commissioner's "Data breach notification guide: a guide to handling personal information security breaches"

NDB Act

The Act and Australian Privacy Principles (Schedule 1 of the Act)

Appendix A – Statement of Notification

PART 1 – *Refer to requirements set out in Section 26WK of the Privacy Amendment (Notifiable Breaches) Act 2017*	
Organisation Name	
Contact Name	
Contact Phone Number	
Address	
Description of the Notifiable Data Breach that Insert Name has reasonable grounds to believe has happened	
Kinds of personal information involved in the data breach	□ Financial Details □ Health Information □ Contact information □ Other Sensitive information □ Other (include details)

Suite 2, 2A Cowper St
Parramatta NSW 2150

Phone: 02 9891 2255
Fax: 02 9806 9731
Email: info@heartbeatnursing.com.au
www.heartbeatnursing.com.au

ABN: 49 084 686 760

Steps that Insert Name recommends that individuals take to reduce the risk that they experience serious harm as a result of this data breach	
Other Entities affected	□ Yes □ No Contact details:

PART 2 – The information that St Elsewhere provides in Part 2 does not need to be included in the notification (s) to affected individuals and Insert Name, may request that it be held in confidence by the OAIC (and insert State Regulatory Body)	
Date the Data Breach occurred	
Date the Data Breach was discovered	
Primary Cause of the Data Breach	□ Malicious or criminal attack □ System fault □ Human error
Description of how the Data Breach occurred	
Number of individuals whose personal information was involved in the data breach	

Suite 2, 2A Cowper St
Parramatta NSW 2150

Phone: 02 9891 2255
Fax: 02 9806 9731
Email: info@heartbeatnursing.com.au
www.heartbeatnursing.com.au

ABN: 49 084 686 760

Description of any action Insert Name has taken to assist individuals whose personal information was involved in the data breach	
Description of any action taken to prevent reoccurrence	
How does Insert Name 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	
List any other data protection authorities, law enforcement bodies or regulatory bodies that you have reported this Data Breach to.	□ Insert State Regulatory Body □ Other (provide details)