P034 – Data Breach Policy

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Approved: | Comments | Next review date |
| 1.0 | 01/06/2018 |  | 01/06/2020  01/06/2021 |

|  |
| --- |
| Applies to: All staff at First Call Nursing. This includes permanent, casual staff, private contractors and consultants engaged by the First Call Nursing to perform the role of a public official. |
| All staff |

# PURPOSE

The purpose of this policy is to provide guidance to First Call Nursing staff for responding to a breach of First Call Nursing held data.

This policy sets out the First Call Nursing procedures for managing a data breach, including:

* providing examples of situations considered to constitute a data breach
* the steps involved in responding to a data breach
* the considerations around notifying persons whose privacy may be affected by the breach.
* template correspondence for notifying persons whose privacy may be affected by the breach

Effective breach management, including notification where warranted, assists the First Call Nursing in avoiding or reducing possible harm to both the affected individuals/organisations and First Call Nursing, and may prevent future breaches.

# What is a data breach?

A data breach occurs when there is a failure that has caused or has the potential to cause unauthorised access to First Call Nursing data, such as:

* Accidental loss or theft of classified material data or equipment on which such data is stored (e.g. loss of paper records that contain client details, progress notes, feedback reports, mobile phone, laptop)
* Unauthorised use, access to or modification of data or information systems (e.g. sharing of user login details (deliberately or accidentally) to gain unauthorised access or make unauthorised changes to data or client records)
* Unauthorised disclosure of classified material information (e.g. email or text message sent to an incorrect recipient or document posted to an incorrect address or addressee), or personal information posted onto the website without consent
* Compromised user account (e.g. accidental disclosure of user login details through phishing/scams)
* Failed or successful attempts to gain unauthorised access to First Call information or systems
* Computer – malware infection – disruption to or denial of IT services

# POLICY

This policy provides guidance for responding to a breach of Information and First Call Nursing held data.

This policy sets out the First Call Nursing procedures for managing a data breach, including the considerations around notifying persons whose privacy may be affected by the breach.

# PROCEDURE

The Managing Director or Senior Coordinator or Office Manager must be informed of any data breach to ensure the application of this policy and to manage any complaints that may be received as a result of the breach.

There are four key steps required in responding to a data breach:

**1. Contain the breach.**

**2. Evaluate the associated risks.**

**3. Consider notifying affected individuals.**

**4. Prevent a repeat.**

Step 1. **Contain the breach.**

Containing the breach is prioritized by First Call. All necessary steps possible must be taken to contain the breach and minimise any resulting damage. For example, recover the personal information, suspend the activity that lead to the breach.

If a third party is in possession of the data and declines to return it, it may be necessary for the First Call to seek legal or other advice on what action can be taken to recover the data.

Step 2. **Evaluate the associated risks.**

To determine what other steps are needed an assessment of the type of data involved in the breach and the risks associated with the breach is undertaken. Some types of data are more likely to cause harm if it is compromised; for example, personal information and health information.

Factors to consider include:

• **Who is affected by the breach?** First Call’s assessment will include reviewing whether individuals and organisations have been affected by the breach, how many individuals and organisations have been affected and whether any of the individuals have personal circumstances which may put them at particular risk of harm.

• **What was the cause of the breach?** The assessment will include reviewing whether the breach occurred as part of a targeted attack or through inadvertent oversight. Was it a one-off incident or does it expose a more systemic vulnerability? What steps have been taken to contain the breach? Has the data been recovered?

• **What is the foreseeable harm to the affected individuals/organisations?** The assessment will include reviewing what possible use there is for the data. For example, could it be used for identity theft, threats to physical safety, financial loss, or damage to reputation? Who is in receipt of the data? What is the risk of further access, use or disclosure, including via media or online?

Step 3: **Consider notifying affected individuals/organisations**

First Call recognises that notification to individuals/organisations affected by a data breach can assist in mitigating any damage for those affected individuals/organisations and reflect positively on First Call’s reputation.

Notification demonstrates a commitment to open and transparent governance, consistent with First Call’s values. If the data breach creates a real risk of serious harm to the individual, the affected individuals must be notified.

In general, if a data breach creates a risk of harm to an individual/organisation, the affected individual/organisation should be notified. Prompt notification in these cases can help to avoid or lessen the damage by enabling the individual/organisation to take steps to protect themselves.

There are occasions where notification can be counter-productive. For example, information collected may be less sensitive and notifying individuals about a privacy breach which is unlikely to result in an adverse outcome for the individual may cause unnecessary anxiety and de-sensitise individuals to a significant privacy breach.

Factors First Call will consider when deciding whether notification is appropriate include:

• What is the risk of harm to the individual/organisation?

• What steps have been taken to date to avoid or remedy any actual or potential harm?

• What is the ability of the individual/organisation to take further steps to avoid or remedy harm?

• Even if the individual/organisation would not be able to take steps to rectify the situation, is the information that has been compromised sensitive, or likely to cause humiliation or embarrassment for the individual/organisation?

• Are there any applicable legislative provisions or contractual obligations that require First Call to notify affected individuals?

The logistics of notifying affected individuals/organisations will depend in large part on the type and scale of the breach, as well as immediately practical issues such as having contact details for the affected individuals/organisations. Considerations include the following.

**3.1 When to notify**

In general, individuals/organisations affected by the breach should be notified as soon as practicable. Circumstances where it may be appropriate to delay notification include where notification would compromise an investigation into the cause of the breach or reveal a software vulnerability.

**3.2 How to notify**

Affected individuals/organisations should be notified directly - by telephone, letter, email or in person.

Indirect notification – such as information posted on First Call’s website, a public notice in a newspaper, or a media release – should generally only occur where the contact information of affected individuals/organisations are unknown, or where direct notification is prohibitively expensive or could cause further harm (for example, by alerting a person who stole the laptop as to the value of the information contained).

**3.3 What to say**

The notification advice will be tailored to the circumstances of the breach. Content of a notification could include:

• information about the breach, including when it happened

• a description of what data has been disclosed

• assurances (as appropriate) about what data has not been disclosed

• what First Call is doing to control or reduce the harm

• what steps the person/organisation can take to further protect themselves and what First Call will do to assist people with this

• First Call’s contact details for questions or requests for information

• the right to lodge a privacy complaint with the Privacy Commissioner

Step 4: **Prevent a repeat**

First Call will further investigate the circumstances of the breach to determine all relevant causes and consider what short or long-term measures need to be taken to prevent any reoccurrence.

Preventative actions may include a:

* security audit of both physical and technical security controls
* review of policies and procedures
* review of employee training practices; or
* review of contractual obligations with contracted service providers
* complete all documentation.

**Notifying the NSW Privacy Commissioner**

As a matter of good practice, the Managing Director will notify the NSW Privacy Commissioner of a data breach where required and when the circumstances indicate that it is appropriate to do so.

Notification should contain similar content to that provided to individuals/organisations. The personal information about the affected individuals is not required. It may be appropriate to include:

• a description of the breach

• the type of personal information involved in the breach

• what response has made to the breach

• what assistance has been offered to affected individuals

• the name and contact details of the appropriate contact person, and

• whether the breach has been notified to other external contact(s).

# FORMS-Template

D034 Data Breach Template V1