Data Breach

POLICY AND PROCEDURE

Purpose

This policy provides a framework that sets out the roles and responsibilities involved in managing a data breach. It also describes the steps an entity will take if a data breach occurs.

Legislation

Privacy and Personal Information Protection Act 1998
Privacy Act 1988 (Privacy Act)
Australian Privacy Principles (APPs)

Definition

Data Breach: A data breach is the intentional or unintentional release of secure or private and confidential information to an untrusted environment.

Personal Health Information (PHI) can include:

The individual's past, present, or future physical or mental health condition (anything that describes the person's condition, such as a diagnosis, examination notes, intake forms, lab test results, etc.)

The provision of healthcare to the individual (anything about any type of treatment the person has had or will have in the future, such as treatment records, prescription information, referrals to other providers, labs that have been ordered, etc.)

The past, present, or future payment for the provision of healthcare to the individual (anything about how the person paid for their care or will pay in the future, such as insurance ID numbers, insurance claim information, check or credit card information, etc.) –

Information that identifies the individual or there is a reasonable basis to believe it can be used to identify the individual (anything a determined person could use to identify somebody, such as birthdate, city of residence, photographs of the person, physical description of the person, etc.)

Information in any format that identifies an individual (e.g., digital files, paper forms, or even voicemail messages/phone calls that could be heard by someone other than the intended party)

PHI Security Guidelines

Security Guidelines requires that when you send any electronic PHI to an individual, you:
1. Send it securely (i.e., use encryption or a portal that requires a login)
2. Believe that it will be delivered to the correct person

Keeping Mobile Devices Secure

- Use a password that follows the guidelines set by IT
- Use and enable message encryption
- Disable and do not use file sharing applications
- Use security software
- Use a firewall
- Keep your security software updated
- Keep your device in your physical control • Use adequate security when using public Wi-Fi, or avoid public networks altogether
- Turn off Bluetooth
- Register your device

Computer Safety

Lock up your computer screen before you walk away

subee
In-Home Care • NDIS Disability Support • Aged Care • Packages

Subee Unit 2, 84-90 Industrial Drive, Coffs Harbour NSW 2450
02 6651 3153 | **www.subeenewlake.com.au**
subee@subeenewlake.com.au

newlake
In-Home Care • NDIS Disability Support • Aged Care • Packages

Newlake 3/11 Glenwood Drive, Thornton NSW 2322
02 4966 8399 | **www.subeenewlake.com.au**
newlake@subeenewlake.com.au

• Never share your login information or passwords with anyone
• File away paper records containing personal information in a locked cabinet
• Leave it in the office, avoid working with PHI outside of the office, especially in public locations where it could be viewed by other—like restaurants, public transit, etc.
• Be vigilant about emails. Clicking an unfamiliar link or attachment could download a virus
• Contact IT and follow established protocols if something suspicious shows up in your inbox
• Back up all files on a regular basis according to company IT policy
• Run updates on all software when prompted to do so

Notifiable Data Breaches

Subee Newlake will respond to data breaches in line with their obligations under the Privacy Act 1988.

Subee Newlake will notify the effected individuals and the commission of certain data breaches.

A notifiable data breach occurs when the following criteria are met:
• There is unauthorised access to or disclosure of personal information held by an entity (or information is lost in circumstances where unauthorised access or disclosure is likely to occur).
• This is likely to result in serious harm to any of the individuals to whom the information relates.
• The entity has been unable to prevent the likely risk of serious harm with remedial action.

Subee Newlake will conduct an assessment if it is not clear if a suspected data breach meets these criteria. The assessment will determine whether the breach is an 'eligible data breach' that triggers notification obligations.

Open Disclosure

All affected individuals will be informed if a data breach occurs.
-If a data breach occurs management is to be notified immediately.
-An incident report is to be completed.
-Management is to promptly contact the affected individuals and other relevant entities.
-If a notifiable breach the appropriate commission will be notified.
- Evaluate how the data breach occurred
- A review of Subee Newlake systems will occur to minimise another breach of data occurring.
- An action plan will be developed including strategies to identify and address any weaknesses in data handling that contributed to the breach.

Training

Subee Newlake undertakes to provide training to all staff.

Staff induction includes:
- access and education around the organisations Privacy Policy, Confidentiality Policy and Data Breach Policy.
- completing the Ausmed e-learning module Keeping Secrets: The health care worker's duty of confidentiality.

subee
In-Home Care • NDIS Disability Support • Aged Care • Packages

Subee Unit 2, 84-90 Industrial Drive, Coffs Harbour NSW 2450
02 6651 3153 | **www.subeenewlake.com.au**
subee@subeenewlake.com.au

newlake
In-Home Care • NDIS Disability Support • Aged Care • Packages

Newlake 3/11 Glenwood Drive, Thornton NSW 2322
02 4966 8399 | **www.subeenewlake.com.au**
newlake@subeenewlake.com.au