Data breaches

Last edited: 22 Feb 2023, 10:59 AM

Introduction

Data breaches are serious situations that have the potential to harm participants, workers and our organisation due to the leaking of sensitive information (such as personal identification numbers, health information and financial information).

Our organisation is committed to having robust mechanisms in place to prevent data breaches and we will establish a planned approach to address any real or suspected breaches of data.

Applicability

When
- applies at all times.

Who
- applies to all workers.

Regulations relevant to this policy

- NDIS (Quality Indicators) Guidelines 2018 (Cth)
- Privacy Act 1988 (Cth)

Preventing data breaches

To prevent data breaches, our organisation will:

- always respect the privacy and dignity of all participants
- ensure that all methods of data collection, both online and offline, have robust security measures in place
- verify the security measures of all third-party information management systems/digital platforms that we are using
- have risk management plan or data breach response plan in place that cover key strategies to mitigate cyber security incidents
- provide training to all workers that covers:
    - data collection and handling
    - data access and editing
    - data deletion and disposal
    - common data security, risks and scams (e.g. phishing emails, fake websites, technical support scams.)
    - key data protection practices (e.g. log in credentials, multi-factor authentication, system updates, anti-virus software, data-backups)
    - steps to take during a data breach incident
    - data breach reporting obligations
- ensure participants feel supported to access their data and provide feedback around our data handling

- only provide participant data to workers and other external parties (e.g. health service providers) that need access to this information
- comply with the following relevant policies:
    - Privacy and Confidentiality
    - Information security
    - Maintenance, records and audit
- comply with all relevant regulations and legislation including:
    - The Privacy Act 1988 (Cth)
    - Australian Privacy Principles (APP)
    - Legislation and regulations relevant to our state
- incorporate data safety into the governance of our organisation.

Reporting data breaches

Under the Notifiable Data Breach (NDB) Scheme, all notifiable data breaches must be reported to the Office of the Australian Information Commissioner (OAIC). A notifiable data breach is any breach of data that is likely to cause any person or organisation serious harm. Examples of serious harm include:

- identity theft
- risk of physical harm
- serious psychological harm
- harm of an individual's reputation
- loss of trust in our organisation
- financial loss
- legal and regulatory consequences.

In addition to the above, we must inform that NDIA at privacy@ndis.gov.au if participant information was compromised during a data breach. This includes participant ID, name and any other identifying information about a participant or their plan.

If a data breach significantly impacts our ability to comply with the requirements of our NDIS registration, we will notify the NDIS Commission.

Managing data breaches

We will take each data breach or suspected data breach seriously and respond immediately to contain, assess and remediate every incident on a case-by-case basis. When responding to a data breach or suspected data breach, we will:

- contain the breach to prevent any compromise of personal information
- assess the breach to gather facts and evaluate risks including potential harm to individuals and whether the breach requires reporting
- act where required to remediate any risk of harm
- notify individuals and (where required) the Office of the Australian Information Commissioner per the requirements of the NDB
- review the incident and consider continuous improvement actions to avoid future breaches.