Supplier Information Sheet: Identifying, reporting and responding to data breaches

What is this information sheet about?

Notifiable Data Breach Scheme

The 'Notifiable Data Breach Scheme (NDB) commences on 22 February 2018.

The NDB Scheme sets out the obligations for notifying affected individuals and the Office of the Australian Information Commissioner (OAIC) about a data breach which is likely to result in *serious harm.*

The NDB Scheme strengthens the existing protections for personal information.

Why is it important?

Baptcare has privacy obligations which are governed by legislation and the Act and we must comply with the NDB Scheme.

As a supplier of services to Baptcare, you must also comply with the legislation and the Act and failure to comply is a breach of your contract with us.

It is important that all suppliers who handle private and sensitive information for Baptcare are able to identify and respond to data breaches and to notify Baptcare immediately they become aware of an eligible data breach.

What is an eligible data breach?

An eligible data breach occurs when the following three criteria are present:

1. There is unauthorised access to, or unauthorised disclosure of personal information, or loss of personal information that Baptcare holds or you hold in relation to the service that you provide to Baptcare; and
2. This is likely to result in serious harm to one or more individuals; and
3. You have not been able to prevent the likely risk of serious harm with remedial actions.

'Serious Harm' may be psychological, emotional, physical, or reputational.

Supplier Information Sheet: Identifying, reporting and responding to data breaches

What may an eligible data breach look like?

- a laptop, Ipad, mobile phone or a client records is left unattended on public transport or in a vehicle, is lost or is stolen;
- where a staff member takes a photo at work which includes all or parts of documents containing personal information (even if that information is in the background of the image);
- where an email containing personal or sensitive information is sent by carbon copy (CC:) to a large group of recipients (or where blind copy (BC) of email addresses should have been used to protect personal email addresses:);
- paper records being placed in and stolen from insecure recycling or garbage bins;
- where a letter containing personal information of one person is sent to another person;
- databases containing personal information being 'hacked' into or otherwise illegally accessed by individuals outside of Baptcare or you; or
- staff member is accessing or disclosing personal information which they do not need to access to perform the requirements if their role.

What do I do if I identify or suspect there has been a data breach?

You must notify your key contact at Baptcare as soon as you are aware of an issue. You must also notify Baptcare by email at Privacy@baptcare.org.au.