Mandatory notification of data breaches by NSW public sector agencies

A submission to the:
NSW Department of Communities and Justice

Prepared by:
yourtown, 23 August 2019

Authorised by:
Tracy Adams, CEO, **yourtown**

yourtown
let's create brighter futures

Email: research@yourtown.com.au Tel: 07 3867 1324

yourtown services

yourtown is a national organisation and registered charity that aims to tackle the issues affecting the lives of children and young people. Established in 1961, **yourtown's** mission is to enable young people, especially those who are marginalised and without voice, to improve their life outcomes.

yourtown provides a range of face-to-face and virtual services to children, young people and families seeking support. These services include:

- Kids Helpline, a national 24/7 telephone and on-line counselling and support service for 5 to 25 year olds with special capacity for young people with mental health issues
- Employment (including a range of Social Enterprises) and educational programs which support young people to re-engage with education and/or employment, including programs for youthful offenders and Aboriginal and Torres Strait Islander specific services
- Accommodation responses to young parents with children who experience child protection and/or homelessness, and to women and children seeking refuge from domestic and family violence
- Young Parent Programs offering case work, individual and group work support and child development programs for young parents and their children
- Parentline, a telephone and online counselling and support service for parents and carers'
- Mental health service/s for children aged 0-11 years old, and their families, with moderate mental health needs
- Expressive Therapy interventions for young children and infants who have experienced trauma and abuse or been exposed to violence.

Kids Helpline

Kids Helpline (KHL) is Australia's only national 24/7, confidential support and counselling service specifically for children and young people aged 5 to 25 years. It offers counselling support via telephone, email and via real time webchat. In addition, the Kids Helpline website provides a range of tailored self-help resources. Kids Helpline is staffed by a paid professional workforce, with all counsellors holding a tertiary qualification.

Since March 1991, children and young people have been contacting Kids Helpline about a diverse group of issues ranging from everyday topics such as family, friends and school to more serious issues of child abuse, bullying, mental health issues, drug and alcohol use, self-injury and suicide.

In 2018, Kids Helpline counsellors responded to over 140,000 contacts from children and young people across the nation, with an additional 843,753 unique visitors accessing online support resources from the website. During 2018, Kids Helpline made its 8millionth contact response.

Introduction

yourtown strongly welcomes the NSW Government's consideration of the application of a mandatory reporting regime to NSW public sector agencies. The effective collection and management of data is a critical issue for both public and private organisations who have an ethical responsibility, and for many a legal responsibility, to maintain and protect the privacy of their service users.

Given the nature of the work we undertake at **yourtown** and the vulnerability of the clients with whom we work, we take this responsibility very seriously. A data breach of our clients' details could risk their safety – whether that be in relation to them being in care, the threat of family violence or the impact on their mental health – and/or could jeopardise their future outcomes, given the stigma attached to criminal history or drug and alcohol use for example.

We therefore support efforts – whether legislation, policy or guidelines – that Australian and international governments are making to improve data security, prevent data breaches and minimise harm when data breaches do occur. However, as a result of Australia's federated system, the National Data Breaches (NDB) scheme does not apply to all government agencies, and hence state and territory agencies need only report breaches on a voluntary basis. This means that the management of sensitive data about service users, and any data breaches that might result relating to them, is subject to different standards depending on the organisation involved and its location.

It acknowledged that deep and persistent societal issues that impact often the most vulnerable, intersect government departments and service providers and require the provision of integrated, client-centred services underpinned by data systems that support information-sharing. The application of different rules for different organisations is untenable. Indeed, it undermines the very aims of the NDB of fostering greater transparency, accountability and confidence in data collection and management if different organisations are held to different standards of account and have different responses to the same data breach. Hence, we commend the NSW Government for looking at this issue.

In our submission, we set out five principles that we believe the NSW Government should consider in the development of legislation relating to public agencies and mandatory data breaches. This includes that:

1. A mandatory data breach scheme should equally apply to all and legislation should be harmonised across the nation
2. Legislation needs to be simple and encourage and support agencies to report breaches
3. Legislation and guidelines should recognise that all data breaches relating to vulnerable children, young people and families could cause serious harm
4. Legislation needs to consider how government agencies will inform, support and work with vulnerable children and young people about data breaches, including in relation to the possible impacts on them now and in the future, and what they can do to minimise risk and respond to a breach

5. Organisations working with data relating to vulnerable children, young people and families need clear expectations about appropriate staff training in data collection and appropriate data access protocols

yourtown submission

1. A mandatory data breach scheme should equally apply to all and legislation should be harmonised across the nation

Like most organisations, effective data collection and management is an integral part of our work at **yourtown**. Importantly, it helps us; to work, record and monitor the issues that confront the children, young people and families with whom we work and assess their progress; to monitor, evaluate and improve the services we deliver and report on our progress, and to work in a coordinated way with other agencies and services that interact with our clients and to which we refer.

Indeed, recognition continues to increase amongst policy-makers and service providers alike of the benefits of joined-up working and information-sharing when responding to a range of client needs in terms of facilitating seamless care pathways, meeting a client's holistic needs and minimising duplication (of clients retelling their stories for example or providers delivering overlapping support services). In practice, however, a range of different issues (many relating to funding) have prevented the development of an integrated support system that puts client needs at the centre but it is an aspiration that policy-makers and service providers are increasingly determined to achieve. Such a system requires high quality data systems and protocols that support the confident exchange of information by different organisations.

In addition, given some of the services we provide at **yourtown** are government-funded, we are obliged to share the sensitive data that we collect and manage about our clients with government agencies, including state and territory agencies that are not covered by the NDB scheme. With the introduction of the NDB scheme showing that the move from the voluntary to the mandatory reporting scheme resulted in a 712% increase in total data breach notifications compared with the previous 12 months, it can easily be surmised that Australian state and territory public agencies are using different standards to data breach reporting that those organisations covered by the NDB. This clearly undermines the effectiveness of the NDB and its intended objectives.

If Australia is to create an environment for effective data collection, management and breach responses that instils trust and minimises the repercussions of a breach then all players within the system must be bound by the same rules. Furthermore, given the nature of data and that it does not respect geographical boundaries, the same rules should apply across the country. A **national** mandatory data breach scheme would help:

- Organisations (especially national organisations) understand their responsibilities and how the scheme works and when and how to report a breach and what are the consequences if they fail to

- The public to better understand their rights and the responsibilities of organisations who hold their data
- Increase confidence amongst all stakeholders that all organisations are undertaking the same approach to data breaches, and thereby help facilitate data-sharing amongst organisations whose clients would benefit from integrated data systems
- Reduce costs associated with data breach reporting – both for organisations bound to the legislation and in reducing the public financial burden of running the scheme through having one national body and approach only
- Ensure that national and state data on organisations that have breached is shared (to thereby more easily identify and respond to organisations who are struggling with data management)

We therefore encourage the NSW Government to make representations to COAG for the harmonisation of this legislation so that public agencies across the nation are bound by the same rules regardless of their location. However, we understand that coordination at this level can be slow and difficult to negotiate, and in the absence of national legislation covering public agencies in this area, we strongly urge the NSW Government to implement legislation in line with the detail of the existing NDB scheme.

2. Legislation needs to be simple and encourage and support agencies to report breaches

Leading on from the previous principle, we strongly advise that a mandatory breach scheme covering public agencies should encourage and support agencies to report breaches. Penalties relating to the scheme must not deter agencies from reporting breaches, whilst the scheme must be easy to access and understand and not overly time-consuming or costly to follow. This is why we again believe that any legislation covering public agencies must mirror that which applies to non-government organisations currently. If different schemes apply it would be extremely resource-intensive and unnecessarily complex for an organisation such as ours to ensure that we are meeting our obligations. A simple and streamlined scheme would encourage and support organisations operating in this space to make timely and appropriate notifications and responses.

3. Legislation and guidelines should recognise that all data breaches relating to vulnerable children, young people and families could cause serious harm

Much has been made about the introduction of NDB scheme to improve public trust in data collection and management. However, we would emphasise the importance of the critical role it plays in keeping vulnerable children, young people and families safe too.

Contact information can be particularly sensitive especially for those who have been moved into care for their safety and protection. Yet the NDB first year insights report shows that contact information was the most common form of personal information disclosed through data

breaches—it was involved in 86 per cent of notifications.[1] Yet the same report states "loss of contact information may not result in immediate or financial harm in the same way as losing credit card information", clearly underestimating the effects that inappropriate sharing of a contact data could have on some people.

Furthermore, information relating to our clients health, criminal records or history of of drug and alcohol use could have significant impacts on their current and future outcomes if they were breached. Indeed, it must be remembered that more, highly sensitive and personal information is likely to be stored on disadvantaged cohorts of people since they are more likely to access services that record this detail. Given the vulnerability of these clients therefore, we would like to see data breach legislation and guidelines acknowledge and accommodate that there is a serious risk of harm to this cohort when data relating to them is breached to ensure that responses appropriately reflect this risk.

4. **Legislation needs to consider how government agencies will inform, support and work with vulnerable children and young people about data breaches, including in relation to the possible impacts on them now and in the future, and what they can do to minimise risk and respond to a breach**

The immediate and future repercussions of a data breach of information relating to vulnerable children and young people (and their families) may be extremely difficult for them to understand. Indeed, it may be inappropriate to inform them of immediate threats in view of their age, circumstances and/or health and wellbeing. This cohort are also unlikely to know how to report that their data has been breached.

However, it is important that appropriate consideration by policy makers and organisations who record data about children and young people is given in relation to when and how to keep them informed and how to provide them with the support they need to minimise the repercussions of a breach and ensure they are kept safe both mentally and physically in the short and long term.

5. **Organisations working with data relating to vulnerable children, young people and families need clear expectations about appropriate staff training in data collection and appropriate data access protocols**

The NDB's first year insights report identifies that most data breaches – including those resulting from a cyber incident – involved a human element "such as an employee sending information to the wrong person or clicking on a link that resulted in the compromise of user credentials".[2] As preventing data breaches is ultimately the best approach to protecting data and those individuals it relates to, we believe that it is important that strict guidelines are developed for organisations working with data that relates to vulnerable children, young people and families. These guidelines

[1] https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-scheme-12month-insights-report/

[2] https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-scheme-12month-insights-report/

would cover the importance of staff training to help prevent data breaches, as well as information about how to ensure that data is appropriately managed within the organisation, and access given to those staff who have been trained in its management and on a 'need to know' basis. There would be significant economies of scale if Privacy Commissioners produced training modules that organisations could use, which would help them overcome the challenges involved in providing their own training.