information and privacy commission new south wales

Statutory Guidelines

NSW Mandatory Notification of Data Breach Scheme

Guidelines on the exemption for risk of serious harm to health or safety under section 59W

September 2023

Who is this information for?	NSW privacy practitioners seeking information about an exemption for risk of serious harm to health or safety under section 59W
Why is this information important to them?	This Guideline is intended to provide agencies with guidance on the operation of the exemption under section 59W. This provision provides that the head of a public sector agency may decide to exempt the agency from notifying affected individuals if the head of the agency reasonably believes that notification would create a serious risk of harm to an individual's health or safety.

Contents

Guidelines on the exemption for risk of serious harm to health or safety under section 59W

Part 6A of the *Privacy and Personal Information Protection Act 1998* (NSW) (PPIP Act), establishes the Mandatory Notification of Data Breach scheme. Under the scheme, all public sector agencies bound by the PPIP Act must notify the Privacy Commissioner and affected individuals of data breaches involving personal or health information that are likely to result in serious harm unless an exemption applies.

The Privacy Commissioner is empowered under section 59ZI to make guidelines for the purpose of exercising the Commissioner's functions under Part 6A.

These Guidelines, made in accordance with that section of the PPIP Act, are intended to provide agencies with guidance on the operation of the exemption under section 59W. This provision provides that the head of a public sector agency may decide to exempt the agency from notifying affected individuals if the head of the agency reasonably believes that notification would create a serious risk of harm to an individual's health or safety.

These Guidelines supplement the provisions of the PPIP Act. Agencies must have regard to them in accordance with section 59I of the PPIP Act.

Sonia Minutillo

A/Privacy Commissioner

Information and Privacy Commission NSW

September 2023

1. Introduction

1.1 Background

Part 6A of the *Privacy and Personal Information Protection Act 1998* (NSW) (**PPIP Act**), establishes a scheme for the mandatory notification of data breaches by NSW public sector agencies.

Under the Mandatory Notification of Data Breach (**MNDB**) scheme all public sector agencies (**agencies**) bound by the PPIP Act must notify the Privacy Commissioner and affected individuals of data breaches involving personal or health information ("personal information") likely to result in serious harm.[1]

The MNDB scheme requires agencies to have regard to any guidelines issued by the Commissioner when assessing a data breach.[2]

These *Guidelines on the exemption for risk of serious harm to health or safety under section 59W* (**Guidelines**) have been made under section 59ZI of the PPIP Act and are designed to help agencies understand and apply the exemption.

Agencies must have regard to these guidelines however, they are not legal advice. Agencies are encouraged to seek professional advice tailored to their own circumstances where required.

Examples are provided throughout the guidelines. These examples are not exhaustive and should be considered as illustrative only.

1.2 Other resources

These Guidelines are part of a suite of guidelines and resources the IPC has developed to help agencies ensure they have the required systems, processes and capability in place, and should be used in conjunction with the following additional materials which can be found on the IPC website:[3]

- Guide to Preparing a Data Breach Policy
- Guide to managing data breaches in accordance with the Privacy and Personal Information Protection Act 1998 (NSW)
- Guidelines on the assessment of data breaches under Part 6A of the PPIP Act
- Guidelines on the exemption for compromised cyber security under section 59X

2. Exemption if serious risk of harm to health or safety

2.1 Overview

When an eligible breach has occurred the head of the agency or their delegate[4] must take all steps that are reasonably practicable to notify the individuals to whom the information relates or who may be affected by the breach.[5]

---

[1] Section 59B of the PPIP Act provides that, for the purpose of Part 6A, personal information includes health information within the meaning of the *Health Records and Information Privacy Act 2002*.

[2] PPIP Act s 59I.

[3] https://www.ipc.nsw.gov.au/privacy/MNDB-scheme.

[4] Any reference in the Guidelines to the head of an agency also includes their delegate. Section 59ZJ provides that the head of an agency may delegate the exercise of a function under Part 6A to a person employed in or by the agency or a class of person prescribed by the regulations.

[5] PPIP Act s 59N.

Under section 59W, where the head of an agency reasonably believes that notification to affected individuals would create a serious risk of harm to an individual's health or safety, they may exempt the agency from the requirement to notify affected individuals. In deciding whether to apply the section 59W exemption, the head of the agency must:

1. Have regard to these guidelines.[6]
2. Consider whether the harm that may result from notifying the breach is greater than the harm that may result from not notifying the breach.[7]
3. Take account of the currency of the information used to assess serious risk of harm.[8]
4. Not conduct a search of the data held by the agency that was not affected by the data breach to assess the impact of notification, unless they know or reasonably believe the data contains information relevant to determining a serious risk of harm to health or safety.[9] The knowledge or reasonable belief must exist at the time the head of the agency decides to conduct such a search.

An exemption under section 59W may be permanent, temporary or conditional, and the head of the agency must notify the Privacy Commissioner of the exemption and its duration.[10]

The policy intent of the MNDB scheme is to empower individuals, provide transparency, and build trust in agency management of personal and health information. In most cases, notification to individuals affected by a data breach can be presumed to be beneficial, as it empowers those individuals to take steps to protect themselves from the risk of harm. Exemptions to notification are intended to apply only in exceptional circumstances. The Privacy Commissioner expects that exemptions under this section will be tightly framed and exercised for a minimal period of time.

2.2 What is a 'reasonable belief'

In order to apply the exemption under section 59W, the head of the agency must 'reasonably believe' that notification would create a serious risk of harm to an individual's health or safety.

A reasonable belief is a belief that results from the exercise of sound judgement. To justify a reasonable belief the head of the agency must be able to explain, based on the information available to them at the time of the decision, the basis on which the belief was formed. This means being able to articulate the specific risks to particular individuals or groups that notification would create.

2.3 What is a 'serious risk of harm to an individual's health or safety'

Whether notification will 'create a serious risk to an individual's health or safety' is an objective test to be determined from the perspective of the head of the agency and based on the information available at the time of the decision to apply the exemption.

'Health' and 'safety' are not defined terms and take on their ordinary meaning. Health refers to a person's mental and physical wellbeing. Safety refers to freedom from danger, risk or injury.

Determining whether a 'serious risk of harm' is created requires consideration of both the likelihood and consequence of harm to an individual. A high likelihood of substantial detrimental effect to the health or safety of an individual would constitute a 'serious risk of harm'.

---

[6] PPIP Act s 59W(3).

[7] PPIP Act s 59W(2)(a).

[8] PPIP Act s 59W(2)(b).

[9] PPIP Act s 59W(2)(c).

[10] PPIP Act s 59W(4).

However, a lower likelihood may still be considered a serious risk of harm where potential consequences are extremely detrimental to an individual's health or safety. For example, the threshold for application of the exemption may be met where the agency makes an assessment that there is a serious risk:

- that notification will exacerbate the mental health condition of an affected individual.
- of harm to the physical safety of agency staff members – for example where an affected individual has a documented history of actual or threatened violence against staff.
- of an individual disengaging from treatment for a significant or life-threatening medical condition.
- of at-risk individuals disengaging with domestic violence or child protection services in circumstances where the agency is aware that is a real risk of serious physical harm or death to the individual and/or their family if service provision is discontinued.

A serious risk of harm to the health or safety of an individual other than the person to whom the information relates may be a relevant risk for the purpose of section 59W. For example, circumstances may exist where notification would cause a serious risk of harm to the affected individual's spouse or another family member.

Individuals for whom notification would create a serious risk of harm may be a sub-group of those affected by the breach. If the broader group can be notified without creating a serious risk of harm to the at-risk subgroup, the exemption will not apply in relation to notification to the broader group. Systematic risks such as harm to the individual's confidence in a service or system will not usually meet the threshold for this exemption. However, in limited circumstances where notification is likely to damage an individual's trust in an agency to such an extent that they would completely disengage from a medical or other service, the exemption may apply. It is expected that this would only be enlivened in rare, exceptional cases.

2.4 Balancing impacts

When deciding whether to exempt the agency from their notification obligations the head of the agency must consider whether the harm of notification outweighs the harm of not notifying.[11]

Taking into account the policy intent of the MNDB scheme and the starting point that notification to affected individuals is usually beneficial, as it empowers them to take steps to protect themselves, agency heads should only rely on the section 59W exception in the circumstances where the harm from notifying the individual is substantively greater than the harm that may result from failing to notify. An agency must satisfy itself that the harm that may result from notifying is real, substantial and not unlikely to eventuate in practice.

2.5 Actions to mitigate risk

When balancing the impacts of notification or failing to notify, agencies should consider whether there are additional steps that they can take to reduce or manage anticipated harms. If there is a practical means of delivering the notification in a way that will mitigate the risks to an individual's health or safety, the exemption will not apply.

Actions to mitigate risk of harm may include:

- **In person notification and/or provision of support** - if an agency is concerned that receiving a notification might cause significant distress to an affected individual, this may be mitigated by providing notice in person with a support person and clinical staff in attendance.

[11] PPIP Act s 59W(2)(a).

- **Redaction of some information** – an agency should consider whether identified risks could be mitigated by redacting specific information or providing a high-level summary. For example, if a law enforcement officer investigating serious organised crime inappropriately accessed information held about individuals in an organised crime group, it may be open to the relevant agency head to form the reasonable belief that notification would create a real risk of harm to the relevant officer's health or safety. When balancing the relevant impacts, the head of the agency should consider whether notification of the data breach can be provided without identifying the individual officer (and so avoiding the risk to them).
- **Notification to an authorised representative** – in the circumstances where an affected individual lacks decision making capacity, the agency may make the notification to the individual's authorised representative. The notification should include information about the health or safety risks to the affected individual and the services available to support the authorised representative to inform the affected person of the breach after they regain capacity.

The Privacy Commissioner expects that the agency will take all reasonable steps to identify any actions that the agency could reasonably take that would mitigate the harms identified and enable notification to occur.

Where a data breach involves the personal information of a child, notification should generally be made to the child's parent or legal guardian. For minors aged 16 years or older it may be appropriate to make the notification directly to the child.

Where an agency decides that notifying a child aged 16 years or over would result in a serious risk of harm to their health or safety, the agency should consider whether it is appropriate to make notification to the child's parent or guardian rather than exercising the exemption. In these circumstances the notification should be accompanied by information on counselling or support services for the child and their family and factors for the parent or legal guardian to consider before informing their child.

2.6 Currency of information

Before exercising this exemption, the head of the agency must consider the currency of the information relied on in assessing whether notification may create a serious risk of harm to an individual. This is because individuals' vulnerability to harm is dynamic and relative, rather than being a fixed trait, and agency records may be old and reflect a particular moment in time.

If agency records indicate that an individual has a particular characteristic or a situational factor that gives rise to a risk of harm to health or safety as a result of notification, consideration should be given to the age of those records and the likelihood that the individual's circumstances may have changed in the intervening time.

2.7 Searching agency data

The head of the agency is prohibited from conducting or instructing the search of agency data unaffected by the data breach in order to assess the impact of notification, unless they hold a reasonable belief that this data contains information relevant to whether the exemption applies. This ensures that the agency is able to access information relevant to its decision making under s59W whilst balancing the protection of personal information held by the agency and ensuring further data breaches do not occur as a result of the assessment process.

For example:

- It would be reasonable for a mental health service to believe that their current patient records would contain information relevant to the assessment of serious risk of harm to the health or safety of these individuals. A health service provider may also reasonably believe that investigating a reference to 'mental health concerns' would provide insight into the application of this exemption.
- It would be reasonable for a school to believe that information concerning Family Court orders or apprehended violence orders contained in a student's record may be relevant to the assessment of serious risk of harm to the health or safety to the student or their care giver.

Any searches conducted based on a 'reasonable belief' should be targeted and conducted to the minimum extent necessary to validate or dismiss the 'reasonable belief'.

2.8 Requesting information from another agency

It may be appropriate for an agency to seek information from another agency when assessing whether a serious risk of harm to health or safety exists.

An agency should only seek information from another agency in circumstances where they hold a reasonable belief that the information is relevant to whether the exemption applies. Agencies should not seek further information as a routine part of the assessment process or undertake 'fishing expeditions' for information that may justify application of an exemption.

An agency which receives a request should only disclose personal information where it is consistent with the disclosure principle under section 18 of the PPIP Act or where an exemption under the PPIP Act, a Code of Practice or Public Interest Direction applies.

2.9 Determining the duration of the exemption

The head of the agency may decide to exempt the agency from its notification obligations permanently, for a specified period, or until the happening of a particular thing.[12] In keeping with the policy intent of the MNDB Scheme, the exemption should be applied only for the minimum amount of time required to avoid or mitigate the anticipated harm.

Where notification would create a serious risk of harm to an individual's health or safety and the risk cannot be mitigated or removed over time, it may be appropriate to apply the exemption permanently. A permanent exemption should only be granted in exceptional circumstances and where the head of the agency has a high degree of confidence that harm mitigation measures, alternative methods of notification and/or the passage of time will not substantially lessen the risk. For example, a permanent exemption may be appropriate where an affected individual has a persistent, serious mental health condition and a documented history of violence or self-harm.

Where the risk of harm arises from a particular factual scenario or a temporary vulnerability, the head of the agency should consider whether they can apply section 59W only until notice can be delivered safely. For example, if an individual is suffering a mental illness that puts them at risk of causing harm to themselves or others if notified of a breach, consideration should be given to whether that mental illness is episodic or likely to resolve, and whether notification obligations could be deferred until such a time as the individual is well enough to receive notification safely.

2.10 Documenting decision making

Agencies should keep appropriate records of any assessment and decision-making process leading to reliance on an exemption, including accurate records of information and evidence used to support their decision.

[12] PPIP Act s 59W(4).

2.11 Notifying the Commissioner

When relying upon this exemption the head of the agency must, by written notice, notify the Privacy Commissioner of the following:

- the fact that the exemption is relied on
- whether the exemption is temporary or permanent, and
- if temporary, the expected duration of the exemption.

The Privacy Commissioner also expects agency heads to provide, if practicable, the following information with any notice of reliance on the exemption:

- the number of people to whom the exemption is applied
- the total number of people affected by the breach
- the nature of the serious risk of harm to health or safety expected to arise from notification
- an explanation of why the risk arising from notifying affected individuals outweighs the risk of not notifying
- the nature and age of information the agency relied on to form its reasonable belief, and
- whether agency records were searched to assess the impact of notification and the grounds on which the search was authorised.

In providing the above information, agencies should not provide the Privacy Commissioner with the personal information of any affected individuals. It will be sufficient for agencies to provide a high-level summary. The Privacy Commissioner may seek further information should it be required.

2.12 Review

Where the head of an agency has applied an exemption for a specified time period, or until the happening of a particular thing regular review dates should be set to consider whether the exemption can be removed and notice provided, or if the exemption should be permanently applied.

The review should consider:

- whether the health or safety risks identified during the initial assessment remain valid.
- whether the health or safety risks continue to outweigh the risks of not notifying.
- whether the ‘particular thing’ has occurred.
- whether the timeframe of the exemption should be amended.
- whether the exemption should be applied permanently.

Agencies should ensure appropriate records of the review are maintained and that any decisions made during a review are accurately recorded and supported by evidence.

The head of the agency must notify the Privacy Commissioner of any new or varied exemption decisions resulting from a review.

Regular reviews should continue until:

- the risk to health or safety is no longer sufficient to justify exercising the exemption and notification may now be made;
- the ‘particular thing’ has occurred and notification can now be made;
- a decision is made to apply the exemption permanently.

Document information

Identifier/Title:	Guidelines on the exemption for risk of serious harm to health or safety under section 59W
Business Unit:	IPC
Author:	Legal Counsel & Regulatory Advice
Approver:	Privacy Commissioner
Date of Effect:	26 September 2023
Next Review Date:	26 September 2024
EDRMS File Reference:	D23/029111/DJ
Key Words:	MNDB Scheme, data breach, exemption, serious harm, health or safety