



**Mental Health
Commission**



Information Breach Policy

Table of contents

Table of contents	2
1 Purpose	3
2 Scope	3
3 Policy Statement	4
3.1 Data Breach Response Framework	4
3.2 Notification	4
3.3 Data Breach Register	5
3.4 Roles and Responsibilities	5
4 Compliance, Monitoring and Evaluation	5
5 Contact for Enquiries	5

1 Purpose

The purpose of the Information Breach Policy (the Policy) is to establish a consistent, whole of agency approach to the identification, management and reporting of information breaches within the Mental Health Commission (MHC).

This Policy ensures that unauthorised access, use, disclosure, loss or destruction of information is appropriately identified, assessed and managed, and that actions are taken to minimise harm to individuals, mitigate organisational risk, and prevent recurrence.

An information breach occurs when information held by the MHC is accessed, used, disclosed, lost, damaged or destroyed without authorisation. This may occur as a result of human error, system failure, or malicious activity. Examples of information breaches include, but are not limited to:

- physical theft or loss of devices containing personal information
- unauthorised access to personal information by an employee
- unintentional disclosure of personal information due to human error
- disclosure of information to external parties due to insufficient identity verification processes
- unauthorised sharing of funding or service information.

This Policy supports compliance with applicable legislation, including the [Privacy and Responsible Information Sharing Act 2024](#), the [Mental Health Act 2014](#), the [Alcohol and Other Drugs Act 1974](#), [Health Services Act 2016](#), and other relevant laws governing the handling of information. This Policy is mandatory under the MHC Data Governance Framework and applies to all information generated, collected, accessed, used, managed, stored or disclosed by the MHC.

Terminology

The term 'data' generally refers to unprocessed facts, while 'information' refers to data that has been processed in a meaningful way. For the purposes of this Policy, the terms 'data' and 'information' are used interchangeably.

For the purposes of the Privacy and Responsible Information Sharing Act 2024 (PRIS Act), a breach involving personal information may constitute a 'data breach' under the PRIS Act. For operational purposes, the MHC uses the broader term 'information breach' to capture unauthorised access, use, disclosure, loss or destruction of any information held by the Commission.

2 Scope

The Policy applies to all persons whether in paid employment, on contract or undertaking voluntary services for the MHC (hereinafter referred to as employees). This Policy applies to all information held by the MHC, including personal and non-personal information, regardless of format, system or business process. This Policy applies to all suspected and confirmed information breaches.

3 Policy Statement

The MHC is committed to protecting the confidentiality, integrity and availability of all information it holds. The MHC recognises that information breaches whether resulting from human error, system failure, or malicious activity, can compromise the security of information, cause harm to individuals, and undermine public trust.

All information breaches must be identified, assessed and managed in a timely and consistent manner. The MHC will take reasonable steps to minimise the risk of information breaches, reduce the impact of any breach that occurs, and implement measures to prevent recurrence. Where an information breach involves personal information, the MHC will assess whether notification is required or appropriate and will meet its obligations under the PRIS Act.

All employees are responsible for protecting information and must report suspected or confirmed information breaches in accordance with this Policy and supporting procedures.

4 Policy Requirement

The MHC must establish and maintain policies, procedures and processes to effectively identify, manage and respond to information breaches.

All suspected and confirmed information breaches must be managed in accordance with the Information Breach Response Plan and supporting procedures.

Where an information breach involves, or is suspected to involve, a cyber security incident, it must also be managed in accordance with the MHC Cyber Incident Response plan and associated incident response procedures.

The MHC will apply a consistent, risk-based approach to managing information breaches, including:

4.1 Information Breach Response Framework

Information breaches must be managed in accordance with the following framework:

- identify the breach
- contain the breach
- assess the breach
- notify and take action to prevent harm
- review the breach and implement improvements.

Reasonable steps must be taken to preserve relevant records and evidence associated with the breach.

4.2 Notification

Information breaches must be assessed to determine whether notification is required or appropriate.

Suspected cyber security incidents must be reported immediately in accordance with the MHC Cyber Incident Response Plan.

Where an information breach involves personal information, the MHC will assess whether the breach constitutes a notifiable data breach under the PRIS Act and will comply with any applicable notification and reporting obligations. The PRIS Act provides that mandatory reporting requirements for serious data breaches take effect from 1 January 2027.

Detailed notification processes are outlined in the Information Breach Response Plan and operational procedure for Information breaches.

4.3 Information Breach Register

All suspected and confirmed information breaches must be recorded in the Information Breach Register regardless of severity.

The register must include sufficient information to:

- support monitoring and reporting
- inform assessment and decision-making
- identify trends and opportunities for improvement.

4.4 Roles and Responsibilities

The MHC must ensure that appropriate roles and responsibilities are defined to support the effective management of information breaches. Detailed responsibilities are outlined in supporting procedures.

5 Compliance, Monitoring and Evaluation

All employees are required to comply with this Policy and supporting procedures. The MHC monitors compliance with this Policy through appropriate governance, assurance and review activities.

6 Contact for Enquiries

MHC Privacy Officer

PRIS@mhc.wa.gov.au



**Mental Health
Commission**



This document can be made available in alternative formats on request for a person with a disability.

© Mental Health Commission of Western Australia 2026

Copyright to this material is vested in the State of Western Australia unless otherwise indicated. Apart from any fair dealing for the purposes of private study, research, criticism or review, as permitted under the provisions of the *Copyright Act 1968*, no part may be reproduced or re-used for any purposes whatsoever without written permission of the State of Western Australia.