Darling Downs and West Moreton PHN

Corporate Policy

Procedure name:	**Critical Incident Reporting Procedure for Commissioned Service Providers**
Approved by:	Executive Leadership Team
Date Effective:	1 August 2026
Review Date:	Annually from the Date Effective
Reference Number:	TBA
Document Classification:	External

Summary of Revisions

Date of changes	Summary description of changes made	Revised By	Approved by (role)
September 2024	V1.0 Initial draft	ED S&O	ED S&O
July 2026	V2.0 Updated to new template & review	Privacy Officer	ED S&O

Purpose

The purpose of this procedure is to outline responsibilities in the effective management of critical incidents and a process that facilitates the identification, reporting, and evaluation of all reported incidents in a timely and effective manner.

The procedure will promote monitoring, learning, and continuous quality improvement from incidents, including near-miss events and system fractures/failures (including AI system/tools), to mitigate future risk and increase awareness of reporting requirements and related legislation.

Scope

This procedure applies to all PHN contracted service providers, agencies and consultants, and their employees.

Overview

Contracted service providers and agencies must deliver services within a robust clinical governance framework and have effective systems for managing and reporting critical incidents relating to the provision of services. Where service provision is of a non-clinical nature, and a clinical governance framework is not a mandatory requirement, appropriate governance, risk and quality management processes must be in place.

This procedure defines the types of incidents that must be reported to the Darling Downs and West Moreton PHN ("PHN"). It outlines timeframes, recording and process for reporting such activity.

Incident management is the responsibility of everyone within an organisation. This reflects the overall Risk Management Standard (AS/NZS 3100:2018). Effective incident management requires a whole of organisation approach, with clear points of accountability for reporting and feedback at all levels of the organisation.

Critical incidents are to be reported to the PHN through electronic submission of a Critical Incident Report Form. The table below provides timeframes for notifying the PHN following the incident or event.

No identifying information (such as the name of the client) is to be disclosed to the PHN in the process of reporting the incident or event.

Incident Definitions

The criteria for clinical incidents are aligned with the Queensland Department of Health Severity Assessment Codes (SAC) 1 and 2:

- death or likely permanent harm which is not reasonably expected as an outcome of healthcare (SAC1).
- near miss or temporary harm which is not reasonably expected as an outcome of healthcare (SAC2).

Clinical Critical Incident To be reported to the PHN: **SAC1: within 1 business day** **SAC2: within 2 business days**	Any incident involving: **SAC1** • Death or likely permanent harm of a current or recent (discharged within 30 days) client that is not reasonably expected as an outcome of healthcare. • Clinical error causing harm to client – including in a situation where a staff member/ contracted service provider has not acted on an observation or report of significant harm to a child[1].

All other events within 5 working days	• Near miss (clinical error with potential to cause harm but did not actually cause harm). • Disclosure or reporting of situational circumstances that placed a consumer in immediate life-threatening danger. **SAC2** • Serious acts of aggression towards self, consumers, carers, or staff (that may result in physical or psychological harm). other event • Professional misconduct of staff member or contracted private practitioner (including abuse or mistreatment of client, inappropriate relationship with client, breach of privacy or confidentiality which is not as a response to a concern for safety, acting beyond scope of practice).
Non-Clinical Critical Incidents To be reported to the PHN: **SAC1: within 1 business day** **SAC2: within 2 business days** **All other events within 5 working days**	Any incident involving the underlying systems, data protection, technology, and financial governance supporting the funded services (ISO 27001:2022 & ISO 42001:2023 alignment): **SAC1** • Death or likely permanent harm of a person that is not reasonably expected as an outcome. • Near miss (error with potential to cause harm but did not actually cause harm). • Disclosure or reporting of situational circumstances that placed a person in immediate life-threatening danger. **SAC2** • Serious acts of aggression towards self and/or any person/people (that may result in physical or psychological harm). other events Professional misconduct of staff member or contracted party (including abuse or mistreatment, inappropriate relationship, breach of privacy or confidentiality which is not as a response to a concern for safety, acting beyond scope of practice). **Privacy & Security** • Data Breaches & Privacy: Unauthorised access, alteration, loss, or exfiltration of patient personal information (PI) or sensitive digital health records. • Cyber Security & Outages: Ransomware attacks, malicious software, or server outages that disrupt clinical workflows, compromise medical devices, or prevent care delivery. • AI System Failures & Malfunctions: Significant model drift, algorithmic bias, or logic errors in AI systems resulting in discriminatory triaging, diagnostic errors, or unfair service denials.

	• Undisclosed AI Deployment: The unauthorised use of an unapproved AI system (e.g., inputting patient information into public ChatGPT or unmapped third-party software). **Governance** • Financial & Governance Mismanagement: Suspected fraud, misappropriation of allocated public funds, or severe operational non-compliance with the funding contract.
Contracted service provider or agency	An organisation that has an active services agreement with Darling Downs and West Moreton PHN.
Eligible Data Breach **To be reported to the PHN: within 3 business days**	An eligible data breach occurs when: • There is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that a contracted service provider, agency or consultant holds. • This is likely to result in serious harm to one or more individuals, and • The contracted service provider or agency has not been able to prevent the likely risk of serious harm with remedial action. A contracted service provider or agency that suspects an eligible data breach may have occurred must quickly assess the incident to determine if it is likely to result in serious harm to any individual.
Incident reporting	The process by which incident data is reported to the PHN. Any incident reported as SAC1 will be reported to the PHN Chief Executive Officer, Board Chair and relevant funding body.
Incident data	All data submitted by the contracted provider or agency to the PHN, which includes but is not limited to incident details, incident management and outcome. Personal details are not to be provided in the reporting process (only supply deidentified details). Incident data will be electronically stored as per the PHN's Data Governance policy and legislative guidelines.

[1] If there is reasonable suspicion that a child has suffered, is suffering or is at an unacceptable risk of suffering significant harm caused by physical, psychological, emotional or sexual abuse or exploitation or neglect and may not have a parent able and willing to protect them, as per the *Child Protection Act 1999.*

Critical Incident Response Guide

1. Incident occurs and is assessed by the organisation/agency/practitioner ("third party").
2. The third party activates their internal critical incident procedures, including notifying all relevant authorities.
3. As per the reporting requirements specified at the *Incident Definition* section of this procedure, the third party is required to communicate initially by phone or email with the appropriate PHN Program Coordinator and/or relevant Program Director. As soon as practically possible (but within the requisite timeframes). The third party must complete and submit the online Critical Incident Report Form.
   No identifying client information (such as names) is to be supplied to the PHN.

4. The PHN Contracts Team, Program Coordinator or Program Director will respond in writing via email acknowledge receipt of the Incident Report.
5. The Incident Report will be reviewed internally within the PHN to ensure all required information has been provided and is complete. If additional information is required from the third party, the contracts team, Program Coordinator or Program Director will communicate any additional information needs or seek specific information clarity.
6. The PHN will determine whether the outcome is:
    a. Closed – matter has been appropriately managed, and no further actions are required from the PHN, or third party. All documentation and data relating to the reporting of this incident will be securely stored by the PHN. Upon closure of the critical incident case, the PHN will notify the reporter of the reporting closure.
    b. Ongoing/Open – further information required or risk mitigation strategies to combat future occurrences need to be determined/employed.
7. Where a critical incident outcome is Ongoing/Open, the PHN may elect to form an Incident Review team from PHN Leadership Team and any relevant subject matter experts. The purpose of this group will be to:
    a. review the incident and associated information to ensure a comprehensive understanding of the event, any causes (factors) and consequences of the incident.
    b. determine the risk of future incidences of the event.
    c. determine any effects of the incident and any changes employed to mitigate future incidences of the event. Pending the escalation of any issues, the PHN may require access to information that identifies the injured party. This would be determined on a case by case basis and under legal advice.

    d. Incidents may only be closed when the PHN (through the Incident Review Team) are satisfied that any current and/or future risk has been eliminated, mitigated or accepted, and there are no further actions required by any of the associated parties.

8. The Chief Executive Officer of the PHN will be notified of any incidents reported and will escalate to the Board as applicable.
9. Documents relating to the reporting of critical incidents will be stored/held in a secure location by the PHN in compliance with applicable statutory requirements.