

Service Provider Safety and Quality Policy

DOCUMENT CONTROL

Managed by: Program Coordinator – Performance Improvement and Evaluation	Approved by: Executive Director of Commissioning	Version: V2.3
Next review date: 03/03/2024	Date approved: 11/05/2023	Status: Approved

REVISION RECORD

Date	Version	Revision Description
1/5/19	V2.0	Updated Detail section
14/4/2020	V2.1	Updated Document Control table; Contents table; minor formatting; and updated link to Report under Associated Documents
18/01/2022	V2.2	Updated link at Associated Documents section Changes to wording to increase clarity, inclusion of a new standard released in 2021
11/05/2023	V2.3	Updated title from Framework to Policy; updated document Control table, added Purpose, added new core standards (ISO 27001) and Clinical Standards (Suicide Prevention Australia Standards for Quality Improvement, 2nd Edition, and Aged Care Quality Standards). Restructure of information and inclusion of Appendix A and B which describe provider self-assessments
17/08/2023	V2.4	Added links to for external access by service providers and regularity of assessment submission

PURPOSE

The intent of this Policy is to communicate the Gold Coast Primary Health Network's (GCPHN's) commitment to quality and safety in commissioning health and human services.

BACKGROUND

Gold Coast Primary Health Network (GCPHN) Service Provider Safety and Quality Policy the 'Policy', aligns with the Core Organizational, Clinical and Service Standards as set by the Australian Safety and Quality Commission or within State Government requirements such as Human Service Quality Framework (Queensland). It has built on the Queensland Government Framework and guiding principles to ensure all non- government agencies funded by the Queensland Government and commissioners ensure:

- Client safety
- Reduction of red tape
- Lessening duplication
- Proportionate response
- Continuous improvement

The Policy guides how GCPHN will ensure that safety and quality for clients by having Service Providers adhered to National and/or State Safety and Quality Standards either through certification against the standards or on completion of self-assessment and annual quality plans to move towards certification and/or improvements in internal systems and processes to reduce key areas of risk.

The Policy is based on recognising the strengths of existing safety and quality standards. It includes thirteen (13) Core Organisation Standards, and six (6) Clinical health standards.

Core Standards (organisational)

1. Corporate governance
2. Service delivery
3. Financial management
4. Consumers
5. Risk, safety and quality management
6. Information, security and privacy management
7. Human resource management
8. Legislative compliance
9. Asset management
10. Continuous quality improvement
11. Diversity responsiveness
12. Transfer of care
13. Building capacity of external community

Clinical Standards

1. Clinical governance
2. Health records management
3. Facilities and equipment management
4. Medication management
5. Infection, prevention, control and management
6. Consumer identification, e.g., for medication administration

DETAIL

Safety and Quality Standards

There are currently four sets of core standards and four sets of clinical standards which are endorsed by GCPHN as meeting the above requirements.

Other standards may be required at GCPHN's discretion dependent on service type and population groups being serviced.

Core Standards (Mandatory)

- Human Services Quality Standards (HSQS)
- National Safety and Quality Mental Health Standards for Mental Health Services (NSMHS 2022)
- QIC Health and Community Service Standards
- National Safety and Quality Primary and Community Healthcare Standards (Certification commencing 2023)

Clinical Standards (Mandatory)

- Royal Australian College of General Practice Standards
- National Safety and Quality Health Service Standards (NSQHS)
- Aged Care Quality Standards

Desired Standards (at discretion of GCPHN)

As deemed appropriate to the safety and quality of service delivery GCPHN may require providers to be accredited to other standards, for example:

- QIP Standards for Safeguarding Children and Vulnerable adults (accreditation program to be widely available in 2023)
- Suicide Prevention Australia Standards for Quality Improvement, 2nd Edition
- Rainbow Tick Standards
- National Safety and Quality Digital Mental Health (NSQDMH) Standards 2020
- ISO 27001 [Information Security Management System]¹ or equivalent

Accreditation requirements for General Practice

General practices are only required to be accredited against the Royal Australian College of General Practice Standards.

Accreditation requirements and self-assessment for all other service providers

All Service Providers who are accredited against any of the Core, Clinical or other Standards specified by GCPHN will be fully or partially exempt from the need to complete the GCPHN self-assessments if accreditation against these Standards is maintained throughout the period of the Service Agreement.

All providers who do not hold any accreditation against the formal Core, Clinical, or other standards as deemed appropriate by GCPHN must complete the following self-assessments

¹ Due to increased risk of cyber security breaches, GCPHN may introduce ISO 27001 to its Core Mandatory Standards from 1 July 2026. Initially all service providers will be required to undertake the Service provider Information Security Assessment to enable GCPHN to determine the most appropriate transition plan. where Service Provider may not have the capacity nor capability to attain ISO 27001 within this timeframe

- [Service Provider Safety and Quality Assessment](#) - a self-assessment by the organisation against the 13 Core Standards detailed above and any of the Clinical Standards relevant to the service type. Additional information about the assessment is included in Appendix A.
- [Service Provider Information Security Assessment](#) a self-assessment by the organisation of its Information Security capabilities and controls to minimise risk of breaches in personal and sensitive data, cybercrime or malicious attack, unauthorised access, misuse of data or reputational damage. Additional information about the assessment is included in Appendix B.

Where a provider is not accredited GCPHN uses a risk-based approach to quality and safety standards, working with the unaccredited service providers to identify the potential areas of greatest risk i.e. client safety, financial, reputation, information security etc. and agree on priorities and timelines to accreditation or and provision of annual quality improvement plan.

Where the Service Provider has already completed a self-assessment for another funder e.g. Queensland Government Department's or PHN, and has an existing quality improvement plan in place, GCPHN will assess the plans to determine if it meets GCPHN requirements. If it does the service provider will not be required to develop a specific annual quality improvement plan for GCPHN and may submit its existing plan to enable GCPHN to monitor development and improvements across the term of the agreement . GCPHN will provide stewardship and support options to assist transition and monitor compliance of providers with prescribed safety and quality standards.

MONITORING IMPROVEMENTS

GCPHN will monitor the risks and quality improvements through.

- Provider reporting and performance meetings.
- Annual Quality Improvement plans, where necessary
- Submission of evidence of accreditation

POLICY REVIEW DATE

This Policy will be reviewed every 1-2 years and in-line with the Policy Review Process.

ASSOCIATED DOCUMENTS

Internal to GCPHN

- [Service Provider Safety and Quality Assessment](#)
- [Service Provider Information Security Assessment](#)

External to GCPHN

- [Service-Provider-Safety-and-Quality-Assessment.docx \(live.com\)](#)
- [Service provider information security assessment \(office.com\)](#)

All Designing and Contracting documents relevant to service providers can be accessed here:

<https://gcphn.sharepoint.com/corporate/QMS/Designing%20and%20Contracting/Forms/AllItems.aspx>

REFERENCES

[Standards | Australian Commission on Safety and Quality in Health Care](#)

[Quality Standards | Aged Care Quality and Safety Commission](#)

[Human Services Quality Framework - Department of Seniors, Disability Services and Aboriginal and Torres Strait Islander Partnerships \(dsdsatsip.qld.gov.au\)](#)

APPENDIX A: SERVICE PROVIDER SAFETY AND QUALITY ASSESSMENT

The Service Provider Safety and Quality Assessment consists of two sections.

1. Overview of Service Provider Safety and Quality Assessment

Gives the provider a general overview of the following 4 Perspectives and the Objectives and Indicators required to be in place for each of the Perspectives:

- Perspective 1: Funded Service Delivery
- Perspective 2: Service User and Community
- Perspective 3: Continuous Quality Improvement
- Perspective 4: Management and Resourcing

2. Service Provider Quality and Safety Assessment: Template

The Report Template provides a reporting tool to enable the Provider to self-assess against 2 - Perspectives.

- Perspective 1: assessed and documented by GCPHN as part of organisation assessment and due diligence
- Perspectives 2-4: are self-assessed by Service Provider

The document can be accessed through the following hyperlink

<https://gcphn.sharepoint.com/corporate/QMS/Designing%20and%20Contracting/Forms/AllItems.aspx>

The assessment report can be accessed for download for completion externally by providers through the following hyperlink

[Service-Provider-Safety-and-Quality-Assessment.docx \(live.com\)](#)

Due: The assessment is to be undertaken and submitted annually, according to the reporting deliverables of Services Agreement.

APPENDIX B: SERVICE PROVIDER INFORMATION SECURITY ASSESSMENT

Information security systems protect an organisation's most important assets, it protects the accessibility, confidentiality and integrity of the systems, data and applications used.

This assessment has been issued by Gold Coast PHN (PHN) to serve as an assessment of the information security controls used by your organisation. The protection of personal and sensitive data is critical. The answers provided in this assessment will help the PHN determine the level of Information Security controls used by your organisation. Any deliberate false answers on this assessment could be treated as a breach of contract or disqualify you from tendering for services.

The document can be accessed internally at GCPHN through the following hyperlink

<https://gcphn.sharepoint.com/corporate/QMS/Designing%20and%20Contracting/Forms/AllItems.aspx>

The assessment can be accessed externally online by providers through the following hyperlink

[Service provider information security assessment \(office.com\)](#)

Due: The assessment is to be undertaken upon execution of the Services Agreement, and annually thereafter, according to the agreed reporting deliverables.