GOLD COAST PRIMARY HEALTH NETWORK PRIVACY POLICY

DOCUMENT CONTROL

Managed by: Information Management	**Approved by:** Director of Commissioning (Systems)	**Version:**
Next review date: 30/06/2021	**Date approved:** TBC 24/04/2020	**Status:** Final

REVISION RECORD

Date	Version	Revision description
12/03/2014	2.0	Updated to the new Australian Privacy Principles
18/03/2014	3.0	Updated to include confidentiality, informed consent and change to the title
01/04/2014	3.1	Correction to list of info held by GCPHN
28/11/14	4.0	Access to ephemeral records
23/05/2017	5.0	Updated with notifiable data breaches
04/04/2019	SharePoint 0.1	Combined Documents – Information Access, Use Management and Privacy Policy and Information Management and Privacy Policy. This document includes Standards and has been updated accordingly.
17/04/2020	SharePoint 1.0	Re-titled to "Privacy Policy" as the Information Access, Use Management and Privacy Policy and Information Management are now included within the Information Management Policy Framework (IMPF); Wording of some sections amended for improved user experience

phn GOLD COAST

An Australian Government Initiative

1. POLICY PURPOSE

The Privacy Act 1988 (the Privacy Act) requires entities bound by the Australian Privacy Principles (APPs) to have a privacy policy. This privacy policy provides detailed information about Gold Coast Primary Health Network's (GCPHN) personal information handling practices and explains how we comply with the Privacy Act. The Privacy Act sets out 13 APPs which regulate how we collect, use, hold and disclose your personal information, and how you may access and correct personal information we hold about you.

2. POLICY SCOPE

This policy applies to all GCPHN operations.

3. POLICY DETAILS

GCPHN handles, holds, and permits access and correction of personal information in accordance with the Australian Privacy Principles, and provides this information for consumers on the website including how to complain about a breach in privacy and request corrections to personal information.

Information Privacy

The Privacy Act defines 'personal information' as:
'information or an opinion about an identified individual, or an individual who is reasonably identifiable whether the information or opinion is true or not; and whether the information or opinion is recorded in a material form or not.'

It will depend on the circumstances as to whether information about you will be considered 'personal information.' For example, information about your name, date of birth or your photos is likely to be considered personal information as you can be identified from this information. Depending on the circumstances, information that does not include your name and date of birth may still be personal information. Note: information does not have to include an individual's name to be personal information. For example, in some cases, a date of birth and post code may be enough to identify a person.

Sensitive information is a subset of personal information. The Privacy Act defines 'sensitive information' as information or an opinion about a person's:

- racial or ethnic origin
- political opinions or membership of a political association
- religious beliefs or affiliations
- philosophical beliefs
- membership of a professional association or trade association
- union membership
- sexual orientation or practices
- criminal record
- health or genetic information
- biometric information and templates.

For example, sensitive information could include a copy of your medical certificate or information about your religion.

The kinds of personal information collected and held by GCPHN

<u>Personal information</u>

GCPHN holds internal information such as employee qualifications and health status, salary information, bank account details, as well as external information such as funding agreements, service provider information and stakeholder information.

Sensitive information

GCPHN does not hold a full patient health record but through certain programs, where informed consent is given, does have access to limited patient information e.g. a referral for services. In these instances, information is treated confidentially with the staff member ensuring the client is aware of the information being recorded, the purpose of recording the information, and which information will be transmitted to other bodies (including funding bodies) and for what purpose. Patient information will only be used for the purposes for which it is collected, unless the information has been de-identified, or consent has been obtained to use it for other purposes. Other sensitive information may be held by GCPHN e.g. professional affiliations or racial or ethnic origin.

Limits to confidentiality

Confidentiality exists between the client and the agency providing the service.
In the following situations, duty of care considerations can override confidentiality:

- when there is an obligation not to conceal an intended or actual crime including child abuse, theft, assault, fraud
- when the client or a third party may be in danger or come to harm if key information is withheld
- when there may be a duty of care consideration to inform a third party

Informed consent

Informed consent means that the client:

- understands the need to exchange personal information about them
- knows what personal information will be exchanged
- knows with whom or what agency the information will be exchanged
- agrees to the exchange
- GCPHN only shares and exchanges personal information with the client's informed consent
- Consent must be recorded on the GCPHN Consent Form which is attached to the client's file

In situations where the worker believes that the client may not have the capacity to give informed consent because of their age, mental state or disability, GCPHN will attempt to get substitute consent from the client's guardian or appointed representative. In situations where the client is unwilling to give consent, the need for privacy will be balanced against the organisation's duty of care responsibilities.

Remaining anonymous or using a pseudonym

You may wish to remain anonymous, or use a pseudonym, when interacting with GCPHN. Where possible, we will allow you to interact with us anonymously or using a pseudonym. For example, we may not need your personal information if you seek general information about a program, policy or consultation process.

However, in some circumstances, it may be impracticable to remain anonymous or use a pseudonym, or we may be legally required to deal with you in an identified form. For example, we may not be able to resolve a complaint that you have made without collecting your name. We will notify you at the time of collection if this is the case.

How GCPHN collects personal information

In most cases, we will collect personal information about you directly from you. However, there may be times when personal information is collected from a third party. If this occurs, such collection will be in accordance with the APPs. As well as collecting personal information directly GCPHN may also collect personal information through other individuals or organisations acting on behalf of GCPHN, including those such as contracted service providers.

When GCPHN collects personal information, we may do this through using forms (either electronic or hard copy), online portals, other electronic or paper correspondence (including emails and written correspondence) and at times verbal conversations or interviews.

When personal information is collected, the individual is issued with a privacy notice explaining the purpose of the collection, the intended use of the personal information and to whom we may disclose it.

Unsolicited information
Unsolicited personal information is provided without it being requested. We may, on occasion, receive unsolicited personal information about you from individuals or other entities, without it being requested.

We will deal with this personal information in accordance with the APPs. That is, we will destroy your personal information unless it is contained in a Commonwealth record or if we consider that we could have lawfully collected it pursuant to the APPs, we may collect it.

How GCPHN holds personal information
GCPHN is considered to 'hold' personal information where it physically possesses a record containing personal information; or has the right to deal with the information, even if it does not physically possess it (such as where the personal information is stored on servers owned by a third party, to which GCPHN has access to, or in archived files).

Under the Privacy Act, we are required to take measures to ensure that when your personal information is to be held by a third party, that the third party complies with the same privacy requirements applicable to GCPHN. GCPHN includes privacy clauses in its contractual agreements with third parties, including funding agreements, consultancy and services contracts and various other ad-hoc contractual agreements. This is to ensure that the third parties handle personal information in accordance with the APPs.

Privacy Impact Assessments (PIA)
GCPHN is required to take reasonable steps to implement practices, procedures and systems that will ensure compliance with the Privacy Act and enable it to deal with enquiries or complaints about privacy compliance.

GCPHN may conduct a PIA for its activities and certain projects. A PIA is an assessment of a project that identifies the impact that the project might have on the privacy of individuals, and sets out recommendations for managing, minimising or eliminating that impact. A PIA may be undertaken in circumstances in which a project involves the handling of personal information. GCPHN must undertake a PIA when directed to do so by the Office of the Australian Information Commissioner (OAIC).

Personal information held by third parties
Under the Privacy Act GCPHN is required to take measures to ensure that when personal information is to be held by a third party, that the third party complies with the same privacy requirements applicable to GCPHN. GCPHN has privacy clauses in all of its legal documents, including funding deeds, services contracts and various other ad-hoc arrangements. This is to ensure third parties that GCPHN deals with are required to handle personal information in accordance with the APPs.

Storage of personal information
Personal information held by GCPHN is stored on electronic media, including cloud computing solutions. Personal information is also held on paper files. Access to records by staff and contractors is restricted to officers on a need to know basis. Our networks and websites have security features in place to protect the information that GCPHN holds from misuse, interference and loss from unauthorised access, modification or disclosure.

Retention and destruction of personal information
We will take reasonable steps to destroy or de-identify your personal information if we no longer need it for the purpose it was collected, unless required by law or a court/tribunal order to retain the information, or if it is contained in a Commonwealth record.

How GCPHN uses and discloses personal information
Unless an exception applies, GCPHN will only use or disclose personal information for the purpose it was collected; and notify the individual of this purpose at the time of collection, or as soon as practicable after collection.

GCPHN will only use or disclose personal information for another purpose where it is able to do so in accordance with the Privacy Act or after receiving consent.

Personal information is used to enable the functions, activities and programs at GCPHN including the functioning of advisory groups, recruitment and HR, maintaining stakeholder relationships, managing funding agreements and contracts, programs and projects, undertaking evaluations and audits, financial transactions, complaints management and research.

Overseas disclosures
GCPHN does not routinely disclose information overseas. Before GCPHN can disclose personal information to an overseas recipient, it will take reasonable steps to ensure that the overseas recipient does not breach the APPs (or recipient's equivalent) and will inform the individual of the countries where the disclosure will occur.

Access and corrections to personal information
GCPHN aims to ensure information it collects uses or discloses is accurate and complete at the time it is collected and will endeavour to keep it up-to-date, e.g. renewing contact details. In the event that you wish to access and/or correct errors in your information, we will take reasonable steps to provide you with access and/or make a correction to your personal information within 30 calendar days, unless we consider there is a sound reason under the Privacy Act or other relevant law to withhold the information, or not make the changes. If we do not provide you with access to your personal information, or refuse to correct your personal information, where reasonable we will:

- provide you with a written notice including the reasons for the refusal
- provide you with information regarding available complaint mechanisms
- at your request, take reasonable steps to associate a statement with the personal information that you believe to be inaccurate, out of date, incomplete, irrelevant or misleading.

If we correct your personal information, at your request, we will also take reasonable steps to notify other agencies or organisations that we have previously disclosed your personal information to, and that are bound by the Privacy Act, of the correction. However, it may not be possible to correct information which has been de-identified, has been published, or there is a legal requirement not to do so. In such instances, you will be informed in writing of the reason why the information cannot be corrected or changed, and the process to make a complaint. Where GCPHN holds ephemeral documents (copies of records e.g. a referral, progress report), if requests are made to access/correct this information, the person will be advised to contact the person/organisation who generated the original record.

4. COMPLAINTS AND PRIVACY BREACHES

If you believe that we have breached the Privacy Act or mishandled your personal information, you can contact our Privacy Officer by phone, mail or our website. Each complaint will be dealt with on a case-by-case basis. All complaints will be investigated by us and you will be advised of the outcome. All privacy complaints are taken seriously.

Procedure for making a complaint
If you believe that we have breached the APPs or mishandled your personal information, you should take the following steps:

1. Contact us: in the first instance, any privacy concern or complaint should be reported directly to GCPHN. This can be done by phone, mail, email or through our website.

2. Submit your concern or complaint in writing: in order to be able to fully investigate your complaint, we would prefer that you make your complaint in writing phone, mail, email or our website. The complaint should include information about the claimed privacy breach and your contact details. Please note that if you do not provide sufficient information, we may not be able to fully investigate and respond to your complaint.
3. Reasonable amount of time: we will acknowledge your concern or complaint upon receipt, if you provide your contact details. We will try to respond to your privacy concern or complaint within 30 calendar days from the date that we receive it. We will notify you if we cannot respond to you within this time period.

Our contact details are:
Telephone: 07 5635 2455
Email: feedback@gcphn.com.au
Post: Privacy Officer, Gold Coast Primary Health Network,
PO Box 3576, Robina Town Centre QLD 4230

If you are not happy with our response, you can complain directly to the OAIC. The Australian Information Commissioner's details are:
Telephone: 1300 363 992
Email: enquiries@oaic.gov.au
Post: Australian Information Commissioner
GPO Box 5218
Office of the Australian Information Commissioner
Sydney NSW 2001

Please note that the OAIC generally requires that a complaint first be raised with us before the OAIC will investigate.

Mandatory Reporting of Notifiable Data Breaches
GCPHN is proactive in protecting its data, implementing data breach response plans and taking steps to protect individuals whose information has been compromised. Where an eligible data breach is suspected, GCPHN is required to provide notification where there are reasonable grounds to believe that an 'eligible data breach' has occurred. An 'eligible data breach' happens where:

- there is unauthorised access to, unauthorised disclosure of, or loss of, personal information held by an entity; and
- the access, disclosure or loss is likely to result in serious harm to any of the individuals whom the information relates.

GCPHN must take reasonable steps to ensure this assessment is completed within 30 days and inform the Office of the Australian Information Commissioner's (OAIC) of any data breaches.

Suggestions
If you wish to make any comments or suggestions about our Privacy Policy or wish to otherwise contact GCPHN in relation to a privacy concern, please contact our Privacy Officer by phone, mail, email or our website.

5. RELEVANT LEGISLATION

Privacy Act, 1988 and Australian Privacy Principles 2014
Notifiable Data Breaches Act 2016
Privacy Amendment (Private Sector) Act 2000
Australian Charities and Not for Profits Commission Act 2012