Privacy policy

Privacy policy

Contents

Privacy policy

1 Introduction

From time-to-time Sunshine Coast Health Network Ltd. (trading as Country to Coast QLD, hereafter **CCQ**) is required to collect, hold, use and/or disclose Personal Information relating to individuals (including, but not limited to its customers, contractors, suppliers and employees) in the performance of its business activities.

The information collected by CCQ will, from time to time, be accessible to certain individuals employed or engaged by CCQ who may be required to use the information in the course of their duties.

This document sets out CCQ's policy in relation to the protection of Personal Information, as defined, under the *Privacy Act 1988 (Cth)* (**the Act**), which includes the *Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth)* and the *Australian Privacy Principles* (**APPs**). The APPs regulate the handling of Personal Information.

The obligations imposed on CCQ under this policy are also imposed on any individual employed or engaged by CCQ.

This policy outlines CCQ's requirements and expectations in relation to the handling of Personal Information. It should be read in conjunction with CCQ's Privacy Management Framework and other CCQ policies and procedures (see Associated Documents).

2 Scope

2.1. Application

This policy applies to all employees, independent contractors, consultants and other workers (**Workers**) engaged by CCQ and who have access to Personal Information in the course of performing their duties.

2.2. Personal Information

Personal Information is information that identifies, or could reasonably be used to identify, a person.

Examples of Personal Information include a person's name, signature, address, phone number, date of birth, sensitive or health information, credit information, employee record information, photographs, internal protocol (IP) addresses, voice print and facial recognition biometrics, location from a mobile device (because it can reveal user activity patterns and habits).

2.2.1. Exclusion of employee record information

This policy does not apply to the collection, holding, use or disclosure of Personal Information that is an employee record as such information is exempt from regulation by the APPs.

An employee record is a record of Personal Information relating to the employment of an employee. Examples of Personal Information relating to the employment of the employee include, but are not limited to, health information and information about the engagement, training, disciplining, resignation, termination, terms and conditions of employment of the employee.

Certain Workers (such as those engaged in a supervisory, operations or human resource capacity) will have access to employee records. Workers who have access to employee records must ensure that the information is handled confidentially and for a proper purpose only. Employee records are only permitted to be collected, used and disclosed where the act of doing so is directly related to a current or former employment relationship.

Workers who may have a question about the use or disclosure of employee records, should contact the Deputy Director Quality, Risk and Compliance.

3 Definitions

Term	Definition
Act	*Privacy Act 1988 (Cth)*
APP Entity	An organisation, business or other agency subject to the *Privacy Act 1988*. This includes some private sector organisations, like the CCQ, as well as most Australian Government agencies.
APP	Australian Privacy Principle/s – these are articulated in Schedule 1 of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012*, which amends the *Privacy Act 1988.*
Data Breach	When Personal Information held by CCQ is subject to unauthorised access or disclosure or is lost.
Entity	See APP Entity.
Express Consent	Consent is given explicitly, either orally or in writing, including handwritten signature, an oral statement, or use of an electronic medium or voice signature to signify agreement.
Notifiable Data Breach	A Data Breach that will likely result in Serious Harm to an individual and CCQ has been unable to prevent the likely risk of Serious Harm with remedial action.
Personal Information	As per definition above in body of policy.
Privacy Notice	APP 5 requires an APP Entity that collects Personal Information about an individual to take reasonable steps either to notify the individual of certain matters or to ensure the individual is aware of those matters. According to the OAIC APP Guidelines, an individual may be notified or made aware of these matters through a variety of formats, provided the matters are expressed clearly. A notice may be prepared in advance (paper, online, telephone script) and staff should be trained to understand their obligation to take reasonable steps to notify or ensure awareness under APP 5.
Sensitive Information	Sensitive Information is Personal Information that includes information or an opinion about an individual's: • racial or ethnic origin • political opinions or associations • religious or philosophical beliefs • trade union membership or associations • sexual orientation or practices • criminal record • health or genetic information • some aspects of biometric information. Generally, Sensitive Information has a higher level of privacy protection than other Personal Information.
Serious Harm	Arising from a Data Breach. May include harm to an individual's physical or mental well-being, financial loss, damage to reputation, identity theft, loss of business or employment opportunities, bullying or marginalisation.
Unsolicited Personal Information	Personal Information that CCQ receives which it did not expressly request.
Worker	CCQ employee, contractor, consultant or other person engaged by CCQ who has access to Personal Information in the course of performing their duties.

4 Policy statement

4.1. Kinds of information that CCQ collects and holds

CCQ collects Personal Information that is reasonably necessary for one or more of its functions or activities or if CCQ has received consent to collect the information.

CCQ's **Privacy Statement**, published on its website, details the types of information CCQ collects from individuals based on the nature of their relationship with CCQ and the purposes for which the information is required.

4.2. How CCQ collects and holds Personal Information

CCQ (and its Workers) must collect Personal Information only by lawful and fair means.

CCQ may collect Personal Information in a number of ways, including without limitation:

i. through forms (e.g. job application, data request, feedback and client intake forms)

ii. by email or other written mechanisms

iii. over a telephone call

iv. in person

v. through transactions

vi. through CCQ website

vii. through lawful surveillance means, such as a surveillance camera

viii. by technology used to support communications, service delivery, research or engagement activities between individuals and CCQ or service providers working with CCQ (for example, Salesforce, Fixus, Microsoft Forms)

ix. through publicly available information sources (which may include telephone directories, the internet and social media sites), and

x. direct marketing database providers.

When CCQ collects Personal Information about an individual through publicly available information sources, it will manage such information in accordance with the APPs.

4.2.1. Privacy Notice

At or before the time or, if it is not reasonably practicable, as soon as practicable after CCQ collects Personal Information, CCQ will take such steps as are reasonable in the circumstances to either notify the individual or otherwise ensure that the individual is made aware of the following:

i. the identity and contact details of CCQ

ii. that CCQ has collected Personal Information from someone other than the individual or if the individual is unaware that such information has been collected

iii. that collection of Personal Information is required by Australian law, if it is

iv. the purpose for which CCQ collects the Personal Information

v. the consequences if CCQ does not collect some or all of the Personal Information

vi. any other third party to which CCQ may disclose the Personal Information collected by CCQ

vii. that CCQ's privacy policy contains information about how an individual may access and seek correction of Personal Information held by CCQ and how an individual may complain about a breach of the APPs, and

viii. whether CCQ is likely to disclose Personal Information to overseas recipients, and the countries in which those recipients are likely to be located.

CCQ's *Privacy Statement*, published on its website, is a generic Privacy Notice that covers CCQ's handling of Personal Information within its standard business activities. This statement may be used as a Privacy Notice where the collection and use of Personal Information is consistent with the information provided in this statement.

4.2.2. Consent to collect Personal Information

Sensitive Personal Information

If CCQ collects **Sensitive Information** (see Definitions), in addition to the collection being reasonably necessary, CCQ will also obtain the **Express Consent** of the individual. The consent must be voluntarily given, either directly by the individual if they have the capacity to give consent, or by someone legally able to act on their behalf. The consent must also be 'current and specific' in nature.

Non-sensitive Personal Information

CCQ does not require an individual's express consent to handle non-sensitive Personal Information, but it does need to reasonably believe that the individual's consent is implied. This is one of the functions of providing a **Privacy Notice** on collection of new Personal Information as it gives individuals the ability to opt-out of the data collection while informing them of the consequences of doing so – e.g., that CCQ may not be able to provide them with required clinical services. Where notified individuals choose not to opt-out, their consent may be taken as implied.

To ensure CCQ Workers collect and manage Personal Information in accordance with the APPs and the best practice recommendations of the Office of the Australian Information Commissioner (OAIC), they should refer to CCQ's *Collecting Consent Procedure* which outlines specifications for the preparation of privacy notices and collecting and recording informed consent from individuals where this is required.

4.2.3. Unsolicited Personal Information

Unsolicited Personal Information is Personal Information that CCQ receives which it did not solicit. Unless CCQ determines that it could have collected the Personal Information in line with the APPs, or the information is contained within a Commonwealth record, it must destroy the information to ensure it is de-identified unless CCQ determines that it is acceptable for CCQ to have collected the Personal Information.

In the CCQ context, Unsolicited Personal Information is typically health data submitted by third parties accompanied by identifying information (name, address, phone number/s or Medicare number) that were not requested by CCQ and received in error, usually via email attachment, fax or hard copy mail.

To ensure CCQ Workers manage Unsolicited Personal Information in accordance with the APPs and the best practice recommendations of OAIC, they should refer to CCQ's *Data Breach and Unsolicited Personal Information Procedure.*

4.3. Use and disclosure of Personal Information

4.3.1. Purposes for using and disclosing Personal Information

Main purposes

CCQ collects Personal Information that is reasonably necessary for one or more of its functions or activities. The main purposes for which CCQ may use Personal Information include, but are not limited to:

i. clinical service delivery, including intake, triage and care coordination
ii. employee recruitment, payroll and human resource management functions
iii. disseminating information, support and engagement activity with CCQ stakeholders
iv. marketing and promotion of CCQ services, training and events
v. contract management and performance monitoring
vi. compliance with funding agreements
vii. paying vendors and suppliers
viii. quality assurance, audit and risk management
ix. conducting surveys and general research, and
x. business and stakeholder relationship management.

CCQ may also collect, hold, use and/or disclose Personal Information if an individual consents, or if required or authorised under law.

Direct marketing

In addition to the above purposes, CCQ may use or disclose Personal Information about an individual (other than Sensitive Information) for the purpose of direct marketing (for example, advising a customer about new goods and/or services being offered by CCQ).

CCQ may use or disclose Sensitive Information about an individual for the purpose of direct marketing if the individual has consented to the use or disclosure of the information for that purpose.

An individual can opt out of receiving direct marketing communications from CCQ by contacting CCQ in writing or, if permissible, accessing CCQ's website and unsubscribing appropriately.

4.3.2. Disclosure of Personal Information

CCQ may disclose Personal Information for any of the purposes for which it is was collected as per the privacy notification made to the individual, or where it is under a legal duty to do so.

Disclosure to third parties

In certain circumstances, CCQ may disclose personal information (or permit third parties to disclose personal information on its behalf) to service providers and other third parties that provide products and services to or on behalf of CCQ. Consistent with APP6, CCQ will only disclose personal information to a third party with the consent of the individual and for the express purpose for which the information was collected.

The main exception to this rule is when CCQ is compelled by law or duty of care to disclose personal information – for example, when an immediate threat or risk of harm to an individual is identified.

Where an individual chooses not to give consent for the disclosure and use of their information to a third party, this may result in limited access to CCQ services and programs.

The organisations or entities to which CCQ may disclose personal information, with an individual's consent, are noted in the table below.

Organisations or entities to which CCQ may disclosure Personal Information
Commonwealth and state government agencies and other funding bodies
External payment system operators and payment verification services.
Legal or government entities to comply with a legal request for an individual's personal information – for example, a subpoena or warrant
CCQ agents, contractors and external advisers
CCQ-commissioned service providers for the purpose of service delivery

Cross-border disclosure of Personal Information

CCQ may on occasion disclose Personal Information to overseas recipients. Before an employee on behalf of CCQ discloses Personal Information about an individual to an overseas recipient, the employee must take steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the APPs in relation to the information.

4.4. Access to Personal Information

If CCQ holds Personal Information about an individual, the individual may request access to that information by completing the Information Access Request form on CCQ's website. CCQ will respond to any request within a reasonable period, and a charge may apply for giving access to the Personal Information where CCQ incurs any unreasonable costs in providing the Personal Information.

There are certain circumstances in which CCQ may refuse to grant an individual access to their Personal Information. In such situations, CCQ will provide the individual with written notice that sets out:

i. the reasons for the refusal, and

ii. the mechanisms available to the individual to make a complaint.

If a Worker receives such a request, they should direct the individual, or their representative, to complete the Information Access Request form via CCQ's website. The Deputy Director Quality, Risk and Compliance will then manage the request in accordance with CCQ's *Information Access Requests Procedure*.

4.5. Correction of Personal Information

If CCQ holds Personal Information that is inaccurate, out-of-date, incomplete, irrelevant or misleading, it will take steps as are reasonable to correct the information.

If CCQ holds Personal Information and an individual makes a request in writing to CCQ to correct the information, CCQ will take reasonable steps to correct the information and CCQ will respond to any request within a reasonable period.

There are certain circumstances in which CCQ may refuse to correct the Personal Information. In such situations CCQ will give the individual written notice that sets out:

i. the reasons for the refusal, and

ii. the mechanisms available to the individual to make a complaint.

If CCQ corrects Personal Information that it has previously supplied to a third party and an individual requests CCQ to notify the third party of the correction, CCQ will take reasonable steps to give that notification, unless impracticable or unlawful to do so.

If Workers receive such a request and are not responsible for managing the relevant data collection, they should refer the request to the appropriate data manager, or if unknown, contact the Deputy Director Quality, Risk and Compliance.

4.6. Integrity and security of Personal Information

CCQ will take such steps (if any) as are reasonable in the circumstances to ensure that the Personal Information that it collects is accurate, up-to-date and complete.

Workers must take steps as are reasonable in the circumstances to protect Personal Information collected and held by CCQ from misuse, interference, loss and from unauthorised access, modification or disclosure.

4.7. Destruction or deidentification of Personal Information

If CCQ holds Personal Information and it no longer needs the information for any purpose for which it may be used or disclosed, and the information is not contained in any Commonwealth record and CCQ is not required by law to retain the information, it will take such steps as are reasonable in the circumstances to destroy the information or to ensure it is de-identified.

If a Worker is unsure whether to retain Personal Information, they should contact the Deputy Director Quality, Risk and Compliance to discuss.

4.8. Data Breaches and Notifiable Data Breaches

4.8.1. Definitions

A **Data Breach** occurs where Personal Information held by CCQ is accessed by, or is disclosed to, an unauthorised person, or is lost. A Data Breach may be caused by malicious action (by an external or internal party), human error, or failure in information systems or security systems. Examples of Data Breaches include:

i. lost, stolen or insufficiently secured technology (e.g. laptops, tablets, mobile phone devices, USB data storage devices, systems and login credentials)

ii. lost or stolen paper records or documents containing Personal Information relating to the CCQ's customers or employees

iii. employees mistakenly providing Personal Information to the wrong recipient (i.e. payroll details to wrong address)

iv. unauthorised access to Personal Information by an employee

v. Workers providing confidential information to CCQ's stakeholders

vi. credit card information lost from insecure files or stolen from garbage bins

vii. where a database has been 'hacked' to illegally obtain Personal Information, and

viii. any incident or suspected incident where there is a risk that Personal Information may be misused or obtained without authority.

ix. Sharing or forwarding Personal Information where CCQ was not the intended recipient or should not have received the information to other parties (for example a patient referral or a service provider report inappropriately containing consumer details).

A **Notifiable Data Breach** occurs where there is an actual Data Breach, and:

i. a reasonable person would conclude that the unauthorised access or disclosure would likely result in **Serious Harm** to the relevant individual (including harm to their physical or mental well-being, financial loss, damage to reputation, identity theft, loss of business or employment opportunities, bullying or marginalisation), or

ii. in the case of loss (i.e. leaving an unsecure laptop containing Personal Information on a bus), unauthorised access or disclosure of Personal Information is likely to occur as a result of the Data Breach, and a reasonable person would conclude that the unauthorised access or disclosure would likely result in **Serious Harm** to the relevant individual (including harm to their physical or mental well-being, financial loss, damage to reputation, identity theft, loss of business or employment opportunities, bullying or marginalisation).

A Notifiable Data Breach does not include a Data Breach where CCQ has been successful in preventing the likely risk of Serious Harm by taking remedial action.

4.8.2. Responding to Data Breaches and Notifiable Data Breaches

Reporting

If a Worker becomes aware of or reasonably suspects a Data Breach, they must report it as soon as reasonably practicable and not later than 24 hours after becoming aware of the actual or suspected Data Breach.

All Data Breaches, suspected or actual, are to be reported via the Internal Information Security and Data Breach Notification form. This notification will trigger the organisation's Data Breach response process, detailed in CCQ's *Data Breach and Unsolicited Personal Information Procedure*.

Assessment

If CCQ is aware of any actual or suspected Data Breach, it will conduct a reasonable and expeditious assessment to determine if there are reasonable grounds to believe that the Data Breach is a Notifiable Data Breach or not.

Notification

Subject to any restriction under the Act, in the event that CCQ is aware of a Notifiable Data Breach, it will, as soon as practicable, prepare a statement outlining details of the breach and notify:

i. the individual whose Personal Information was part of the Data Breach, and

ii. the Office of the Australian Information Commissioner.

4.9. Anonymity and pseudonymity

Individuals have the option of not identifying themselves, or using a pseudonym, when dealing with CCQ in relation to a particular matter. This does not apply:

i. where CCQ is required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves, or

ii. where it is impracticable for CCQ to deal with individuals who have not identified themselves or who have used a pseudonym.

However, in some cases if an individual does not provide CCQ with the Personal Information when requested, CCQ may not be able to respond to the request or provide them with the goods or services that they are requesting.

4.10. Privacy complaints

Individuals have a right to complain about CCQ's handling of Personal Information if the individual believes CCQ has breached the APPs.

If a Worker becomes aware of an individual wanting to make such a complaint to CCQ, they should direct the individual to complete the online Feedback Form on CCQ's website. Complaints received will be managed with in accordance with CCQ's *External Feedback Management Policy* and *Procedure*.

Individuals who are dissatisfied with CCQ's response to a privacy complaint, may refer the complaint to the Office of the Australian Information Commissioner.

4.11. Breach of this policy

Workers directed by CCQ to perform an act under this policy which relates to Personal Information, must ensure that in performing the act they comply with the obligations imposed on CCQ. A Worker directed by CCQ who fails to perform an act in accordance with this policy will be deemed to have breached the policy and will be subject to formal counselling and disciplinary action, up to and including possible termination of employment.

5 Roles and responsibilities

Role/Position	Responsibility
Chief Executive Officer (CEO)	• Final decision-maker in relation to CCQ's management of Personal and Sensitive Information.
Director Commissioning – Chief Data Officer	• Oversees CCQ privacy management framework. • Provides SME advice and recommendations to CEO in relation to management of Personal and Sensitive Information as required.
Deputy Director Quality, Risk and Compliance	• Policy owner – responsible for compliance, monitoring, review and receiving feedback in relation to the policy. • Point of contact for Workers in relation to privacy management procedures and processes. • Provides advice and training to Workers regarding the appropriate handling of Personal Information according to the APPs.
Workers	• Awareness of policy and compliance with APPs when handling Personal and Sensitive Information.

6 Associated documents

6.1. Legislation, standards, practice codes, regulatory requirements

- *Privacy Act 1988 (Cth)*
- *Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth).*
- *Australian Privacy Principles*
- AS/NZS ISO/IEC 27001:2006 Information Technology – Security Techniques – Information Security Management Systems – Requirements.
- AS/NZS ISO/IEC 27002:2006 Information Technology – Code of Practice for Information Security Management.
- AS ISO 27799:2011: Information Security Management in Health Using ISO

6.2. CCQ policies, procedures, frameworks

Document number	Document name
FRA-PRI-001	Privacy management framework
STA-PRI-001	Privacy statement (published on CCQ website)
PRO-PRI-001	Data breach and unsolicited personal information procedure
PRO-PRI-003	Collecting consent procedure
PRO-PRI-005	Information access requests procedure
POL-CQI-001	External feedback management policy
PRO-CQI-001	External feedback management procedure
POL-HR-013	Performance counselling and discipline policy
FRA-ICT-001	Knowledge management framework
POL-ICT-003	Identify management policy