Privacy Policy

ONCALL

ONCALL/SACARE[1]'s vision is to be nationally recognised as the leading integrated community service provider, empowering people to live their best lives. ONCALL is steadfastly focused on quality service that puts the client at the centre, is enabled through technology transformation, and delivered by people who are committed.

Quality and compliance are embedded into our daily actions and behaviours. ONCALL's policies and procedures provide the foundation and framework for our work and actions to ensure we provide best practice service quality and compliance. All staff are required to know and apply ONCALL policies and procedures that apply to their work.

Policy Purpose

As a provider of services for people with disability, families, and young people, ONCALL has access to personal information in every interaction and part of our business. Keeping front of mind, assuming all information is personal information, and respecting and protecting individual's privacy and confidentiality in every interaction is critical for ONCALL, its staff, Board, and partner organisations.

This policy covers the entire information lifecycle from collection, security, use and disclosure, access and correction and destruction of all personal information including sensitive and health information.

Adherence to the policy will ensure that everyone who is provided services by, works for, or works with, ONCALL is guaranteed that their personal information will be collected and managed as required by legislation and that ONCALL meets client expectations, and delivers on our values of respect, accountability, and service excellence.

ONCALL has no tolerance for any intentional breach of privacy. Serious legal, professional, and financial impacts and penalties apply to intentional breaches of privacy.

ONCALL Privacy Policy adheres to applicable Commonwealth and state legislation for the management of personal including health information:

- Privacy Act 1988 (Cth) (the Privacy Act)
- Privacy and Data Protection Act 2014 (Vic)
- Health Records Act 2001 (Vic)
- Victorian Charter of Human Rights and Responsibilities Act 2006 (Vic)
- Fair Work Act 2009 (Cth)
- Human Rights Act 2019 (Qld)
- National Disability Insurance Scheme (NDIS) Quality and Safeguarding Framework 2017 (Cth)

Policy Scope

This policy applies to the management of client personal information by all ONCALL staff including contractors and consultants, partner organisations, and Board members.

Policy Statement

ONCALL has adopted the Australian Privacy Principles (APPs) as contained in Schedule 1 of the Privacy Act 1988, the Victorian Information Privacy Principles (IPPs) contained in Schedule 1 of the Privacy and Data Protection

[1] ONCALL is inclusive of the following entities - ONCALL Group Australia; Ablecare Pty Ltd trading as ONCALL; SACARE Pty Ltd. Throughout this document, ONCALL/SACARE will be referred to as ONCALL.

Act 2014 (Vic) and the Health Privacy Principles (HPPs) as contained in Schedule 1 of the Health Records Act 2001 (Vic). The legislation and principles set out ONCALL's obligations and individuals' rights around:

- the collection, use and disclosure of personal information.
- an organisation or agency's governance and accountability
- integrity and correction of personal information
- the rights of individuals to access their personal information

Application of Privacy Principles

Collection

It is an individual's right to choose whether to share personal information. If an individual (client or staff member) chooses not to share personal information required for ONCALL to deliver its service or function, ONCALL may not be able to provide some services or to commence or maintain their employment of a staff member.

ONCALL will only collect personal information where it is necessary for one or more of its functions or activities. The information will be collected lawfully and fairly and not in an unreasonably intrusive way.

Personal information collected may include:

- an individual's name, signature, address, phone number or date of birth
- sensitive information
- credit information
- employee record information
- photographs
- internet protocol (IP) addresses
- voice print and facial recognition biometrics
- location information from a mobile devi

Health information collected for a potential or current client may include:

- personal health history and family history
- lifestyle, cultural or ethnic background
- test results to assist in providing appropriate support

ONCALL will, as far as practicable and reasonable, collect personal and health information about an individual only from that individual. If required to be collected from someone else, ONCALL will take reasonable steps to ensure that the individual is advised of its collection and management as consistent with privacy principles.

ONCALL will take all reasonable steps to ensure that the personal information collected, used, or disclosed is accurate, complete, and up to date.

Security

ONCALL will take reasonable steps to protect personal information it holds is stored in a manner that reasonably protects it from misuse and loss and from unauthorised access, modification, or disclosure. ONCALL will not adopt as its own identifier an identifier that has been assigned by a government agency (or by the government's agent or contractor).

ONCALL security measures include holding personal information in electronic form in secure databases owned and operated by ONCALL and by measures including firewalls, SSL data encryption, virus detection methods, and password restricted access.

ONCALL adheres to Australian data sovereignty requirements that data is kept in a data centre physically located in Australia and is only accessible by Australian people and companies. ONCALL will only transfer personal or

confidential data outside of Australia if the transfer is for the benefit of the individual concerned or is necessary for the conclusion or performance of a contract AND that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds Australian Privacy Principles.

Use and Disclosure

The personal information disclosed to ONCALL by staff or clients will be used:

- for the purposes for which it was collected
- for other related purposes for which the individual would reasonably expect ONCALL to use the information including providing to persons/offices having legal authority to access personal information
    - some of the services provided within or by ONCALL may be outsourced or provided by a contractor (i.e. physiotherapists or outpatient services). ONCALL may provide personal information to them to assist in providing support and care. Further, if an individual requires certain medical devices for treatment, ONCALL may disclose personal information to suppliers or manufacturers of those devices. ONCALL requires all such health professionals and contractors to handle personal information in accordance with the Privacy Act
- if the personal information is sensitive information, the secondary purpose is directly related to the primary purpose of collection
- where it is required or permitted by law to do so for other related purposes to which the individual has agreed (either expressed or implied). This may include providing the user with details about other goods or services offered by ONCALL, as well as any newsletters, promotions, surveys, or staff training, if applicable. In these instances, ONCALL will provide options for a client to request not to receive direct marketing (opt out)
- from time to time, we may need to collect, use or disclose aspects of your personal information to monitor the standard of services provided, through processes such as accreditation and evaluation, clinical audits, risk and claims management, education and training of staff, and quality assurance activities, including monitoring clinical outcomes
- to ensure we are delivering our services to meet our participant's needs, we monitor participant satisfaction. As a result, we, or someone we authorise, may contact you in the future to request your feedback on our services
- ONCALL collects, uses and discloses personal information about its staff in order to perform its obligations as an employer and as required by law. However, the handling of past and current employee records is exempt from the Privacy Act where there is a direct relationship between ONCALL and the past/current employee. ONCALL will retain employee records confidentially and in accordance with the Fair Work Act 2009 (Cth) which sets out entitlements in relation to these documents

Access and Correction

ONCALL will provide a privacy statement to all clients. The privacy statement documents ONCALL policy on the management of personal information including how to correct and update their personal information.

ONCALL will provide individuals with access to their personal information if requested unless the request meets one of the exceptions listed in any of the information or health privacy Principles. Access to personal information should be requested from AskQuality@oncall.com.au. ONCALL will provide reasons for denial of access or a refusal to correct personal information.

Where ONCALL is not required to provide the individual with access to the information for any allowable exception, ONCALL will, if reasonable, consider whether the use of mutually agreed intermediaries would allow sufficient access to meet the needs of both parties.

If ONCALL levies charges for providing access to personal information, those charges will not apply to lodging a request for access and will not be excessive.

If an individual can establish that the information held by ONCALL is not accurate, complete, and up to date, ONCALL will take reasonable steps to correct the information so that it is accurate, complete and up to date.

If the individual and ONCALL disagree about whether the information is accurate, complete, and up to date, and the individual asks ONCALL to associate a statement to the information claiming that the information is not accurate, complete, or up to date, ONCALL will take reasonable steps to do so.

Data Destruction

When the information is no longer required for service delivery or as required or authorised by law, ONCALL will irreversibly destroy the documents using the same level of security that was maintained during the life of the records, or to permanently de-identify personal information. ONCALL will document record destruction.

Electronic Media and Collection of Personal Information

The Privacy Principles and related legislation apply to the collection and management of personal information acquired through any electronic media platform utilised by ONCALL including ONCALL web site and social media platforms.

The ONCALL website uses 'cookies' that collects information from your website usage. This information is used for website administration, statistical analysis, and maintenance. The information is aggregated and not linked to particular individuals. You are able to adjust your web browser settings to block cookies. Some parts of the ONCALL website may not function fully for users that disallow cookies.

Forms on the ONCALL website may request that you complete personal information such as name or contact details. ONCALL collects this information so that ONCALL can assist you with the query or request you use the form to submit. You are not required to utilise these forms, but ONCALL may be limited in responding if this information is not provided.

Breaches of this Policy

The breach of this policy by a team member, director or officer of the company may lead to disciplinary action being taken in accordance with the company's disciplinary procedure. Serious breaches may be regarded as gross misconduct.

All team members, directors and officers of the company will be expected to cooperate fully in any investigation into suspected breaches of this policy or any related processes or procedures. If an issue is identified with a supplier, we will work with them to prepare a corrective action plan and resolve all violations within an agreed upon time period. We reserve the right to terminate our relationship with individuals and organisations in our supply chain if they breach this policy.

Complaints

Any person interacting with ONCALL who believes (or whose family or significant person believes) that his or her personal information has been managed inappropriately or illegally or have any concerns on the management of their personal information, is encouraged to advise ONCALL. The person may engage an advocate to support them.

ONCALL provides ready access for complaints or feedback by email to AskQuality@oncall.com.au. ONCALL is committed to respecting people's rights to complain and will ensure no adverse consequences of any complaint or feedback.

ONCALL will respond to the complaint or feedback within 3 days and will work with affected individuals to achieve a satisfactory resolution. ONCALL will provide information on access to other complaints bodies if matters are unable to be resolved. ONCALL will record and use all feedback and complaints and use this information to improve its services through its continuous quality improvement cycle.

Definitions

PERSONAL INFORMATION	Personal information includes a broad range of information, or an opinion, which could identify an individual. Personal information may include: an individual's name, signature, address, phone number or date of birth; sensitive information; credit information; employee record information; photographs; internet protocol (IP) addresses; voice print and facial recognition biometrics; location information from a mobile device (because it can reveal user activity patterns and habits) (OAIC)
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 beliefs, sexual orientation or practices, criminal history, health or genetic and some aspects of biometric information (OAIC)
HEALTH INFORMATION	Health information is any personal information about a person's health or disability. It includes information or opinion about their illness, injury or disability. Examples of health information include: • notes of health symptoms or diagnosis; information about a health service used by an individual; specialist reports and test results; prescriptions and other pharmaceutical purchases; dental records; genetic information; a person's wishes about future health services; wishes about potential organ donation; appointment and billing details; any other personal information collected by a health service provider (OAIC)
CONFIDENTIAL INFORMATION	Any information disclosed by an individual, whether orally or in writing, that is, or should reasonably be, understood to be confidential given the nature of the information and the circumstances, or specifically designated as confidential
INFORMATION LIFECYCLE	The information lifecycle is the flow of information from the point the organisation collects the information to the point the information is destroyed. There are five stages of the information lifecycle: Collection; Security; Use and disclosure; Access and correction; and Data destruction (OVIC). Refer *Appendix 3*
ELECTRONIC MEDIA	Electronic media includes, but is not limited to email, internet, intranet, voicemail, instant messaging and chat facilities, and online discussion groups including social media
SOCIAL MEDIA	Social media includes any facility for online publication and commentary. Most forms of social media are interactive, allowing users to create and share content online

Related Documents

Policy, Procedure, Manual

ONCALL Privacy Statement
Charter of Human Rights and Responsibilities Policy
Disciplinary Action Policy
Document Retention and Release Policy

Feedback and Complaints Policy
Social Media Policy
Staff Code of Conduct
Use of Electronic Systems and Communications Policy

Legislation

Fair Work Act 2009 (Cth)
Health Records Act 2001 (Vic)
Human Rights Act 2019 (Qld)
National Disability Insurance Scheme (NDIS) Quality and Safeguarding Framework 2017 (Cth)
Privacy Act 1988 (Cth) (the Privacy Act)
Privacy and Data Protection Act 2014 (Vic)
Victorian Charter of Human Rights and Responsibilities Act 2006 (Vic)

Document Control

Approval and Review

DOCUMENT OWNER	Audit, Compliance and Risk Management Committee (ACRM)		
APPROVAL DATE	November 2023	**REVIEW DATE**	November 2025

Access and Feedback

This policy will be made available to all staff on the ONCALL intranet and ONCALL database (Periscope), and to directors in the ONCALL Board orientation.

Users should provide comments and feedback on the accuracy, currency, and useability of the policy document to AskQualityVic@oncall.com.au.

Appendix 1: Summary Comparison of Australian Privacy Principles, Information Privacy Principles (Vic) and Health Privacy Principles (Vic)

AUSTRALIAN PRIVACY PRINCIPLES (CTH)	INFORMATION PRIVACY PRINCIPLES (VIC)	HEALTH PRIVACY PRINCIPLES (VIC)
APP 1 Open and transparent management of personal information	IPP 1 Collection	Principle 1 Collection
APP 2 Anonymity and pseudonymity	IPP 2 Use and Disclosure	Principle 2 Use and disclosure
APP 3 Collection of solicited personal information	IPP 3 Data Quality	Principle 3 Data quality
APP 4 Dealing with unsolicited personal information	IPP 4 Data Security	Principle 4 Data security and retention
APP 5 Notification of the collection of personal information	IPP 5 Openness	Principle 5 Openness
APP 6 Use or disclosure of personal information	IPP 6 Access and Correction	Principle 6 Access and correction
APP 7 Direct marketing	IPP 7 Unique Identifiers	Principle 7 Identifiers
APP 8 Cross-border disclosure of personal information	IPP 8 Anonymity	Principle 8 Anonymity
APP 9 Adoption, use or disclosure of government related identifiers	IPP 9 Transborder Data Flows	Principle 9 Transborder data flows
APP 10 Quality of personal information	IPP 10 Sensitive Information	Principle 10 Transfer/closure of a health service practice
APP 11 Security of personal information		Principle 11 Sensitive information
APP 12 Access to personal information		Principle 12 Making information available to another health service provider
APP 13 Correction of personal information		

Appendix 2: Australian Privacy Principles (APP)

*To ensure currency documents should be accessed from the source legislation or the website of The Office of the Australian Information Commissioner at www.aoic.gov.au.

PRINCIPLE	TITLE	PURPOSE
APP 1	Open and transparent management of personal information	Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy
APP 2	Anonymity and pseudonymity	Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply
APP 3	Collection of solicited personal information	Outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of sensitive information
APP4	Dealing with unsolicited personal information	Outlines how APP entities must deal with unsolicited personal information
APP 5	Notification of the collection of personal information	Outlines when and in what circumstances an APP entity that collects personal information must tell an individual about certain matters
APP 6	Use or disclosure of personal information	Outlines the circumstances in which an APP entity may use or disclose personal information that it holds
APP 7	Direct marketing	An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met
APP 8	Cross-border disclosure of personal information	Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas
APP 9	Adoption, use or disclosure of government related identifiers	Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier or use or disclose a government related identifier of an individual
APP 10	Quality of personal information	An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure
APP 11	Security of personal information	An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances
APP 12	Access to personal information	Outlines an APP entity's obligations when an individual requests to be given access to personal information held

		about them by the entity. This includes a requirement to provide access unless a specific exception applies
APP 13	Correction of personal information	Outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals

Information Sources

The Office of the Australian Information Commissioner:

- www.aoic.gov.au
- https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-quick-reference

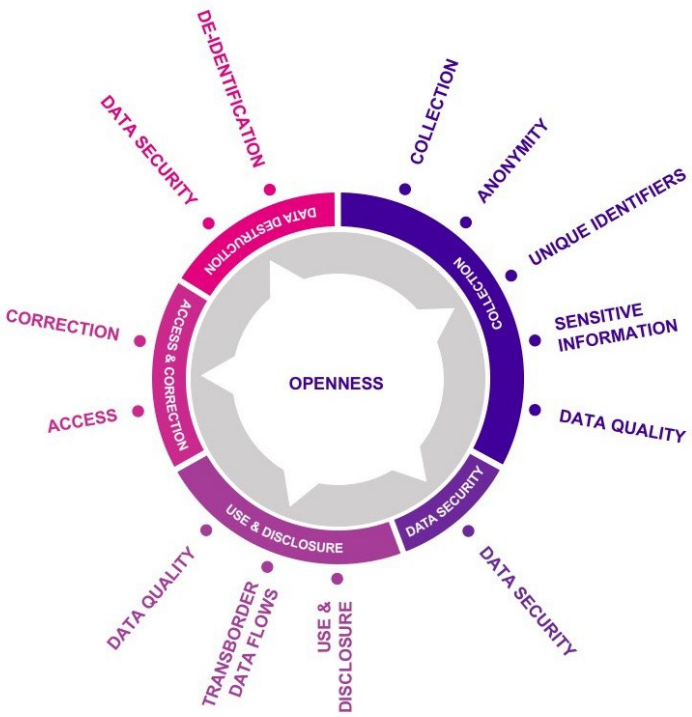
Appendix 3: Information Privacy Principles (IPP) & Information Lifecycle

*To ensure currency documents should be accessed from the source legislation or the website of The Office of the Victorian Information Commissioner:

https://ovic.vic.gov.au/privacy/information-privacy-principles-short-guide/

THE INFORMATION LIFECYCLE

Excerpt from Information Privacy Principles Short Guide



Appendix 4: Health Privacy Principles (HPP)

*To ensure currency documents should be accessed from the source legislation:

https://www.legislation.vic.gov.au/in-force/acts/health-records-act-2001/046

Or, in summary from the Department of Health website:

https://www.health.vic.gov.au/rights-and-advocacy/rights-and-privacy-principles.