

1.0 PURPOSE AND SCOPE

EACH is committed to meeting legislative and regulatory requirements related to protecting and upholding the right to privacy and confidentiality of our customers, our personnel, the organisation, and key stakeholders.

2.0 POLICY STATEMENT

2.1 Introduction

EACH respects the individual's right to privacy of their personal, health and sensitive information. EACH complies with *The Privacy Act 1988 (Ct.)* and the Privacy Principles contained in this Act. EACH is also bound by relevant State and Territory legislation relating to the privacy of health records and information:

- [Health Records Act 2001 \(Vic\)](#)
- [Health Records and Information Privacy Act 2002 \(NSW\)](#)
- [Information Privacy Act 2009 \(Qld\)](#)
- [Health Records \(Privacy and Access\) Act 1997 \(ACT\)](#)

EACH regularly reviews this policy in line with updates and changes to both Commonwealth and State/Territory legislation.

EACH personnel receive orientation to privacy practices and understand their obligations under the [EACH Code of Conduct](#) relating to privacy and confidentiality and always ensure that the privacy of customer and EACH personnel information is protected.

Privacy and confidentiality are to be always respected and in all transactions. EACH:

- Collects only information which the organisation requires for its primary function.
- Ensures people are informed as to why we collect the information and how we administer the information gathered.
- Uses and discloses personal information only for our primary functions or a directly related purpose, or for another purpose with the person's consent.
- Stores personal information securely, protecting it from unauthorised access
- Provides stakeholders with access to their own information, and the right to seek its correction.

2.1.1 Consent

Consent to collect, use, share and disclose personal, health or sensitive information is discussed at varying times from initial contact with EACH through to the ongoing provision of services. Consent is an ongoing process as we check in with customers and personnel from time to time to ensure the information, we hold is current and maintained accurately.

Refer to the [Collection, Use and Sharing of Personal and Sensitive Information Procedure](#)

EACH personnel at the time of collection of customer information discuss privacy in line with [Delivering services with trust and respect brochure](#).

- Why we collect personal, (including health and sensitive) information
- How their personal information is protected
- Require express customer consent to share information with external services

The information a customer provides may be collected, recorded and stored from the initial point of inquiry with implied consent, for example, basic demographic information and reason for inquiry.

2.1.2 Informed Consent

The principles of competence, voluntariness, specificity, and understanding are central to all forms of consent. Consent forms the basis for many privacy expectations of permitting collection, use, sharing and disclosure of personal and sensitive information. Involving customers in decisions about their care and well-being acknowledges their personal worth and individuality as well as their responsibility in managing their own health and wellbeing. Refer to [Informed Consent Procedure](#).

2.1.3 Anonymity

It is the right of an individual not to identify themselves when accessing services from EACH. If a customer chooses not to disclose their identity, the level or type of service that we can offer may be limited.

Most of our services require collection of your personal information as this enables us to provide you with the most appropriate care, support and/or treatment. If a customer does not consent to collection of their personal information, the level or type of service that we can offer is limited. Most of our services require collection of relevant personal information as this enables us to provide the customer with the most appropriate care, support and/or treatment.

2.1.4 Collection

The primary purpose for EACH to collect information is to enable provision of tailored, quality services.

When you contact EACH, all information that you provide is recorded, including from an initial inquiry before receiving an EACH service.

Information is collected in a respectful, lawful, and non-intrusive way. Wherever possible, information is collected directly from the customer. If this is not possible or practical then personal information may be collected from a representative, from a carer or relative or from a third party such as another health service provider. The customer is notified if we have collected information from a third party.

We only collect personal information for purposes that are directly related and necessary to our activities and the services that we provide, and which is essential to the quality and effective administration of our services.

We also collect personal information related to our personnel and others who participate in the functions and operations of EACH. We only collect information necessary to facilitate employment with EACH and meet compliance requirements. All records of a personal and confidential nature are maintained securely, and access restricted to authorised personnel.

2.1.5 Use and disclosure

We only use personal information for the purpose for which it was given to us, or for purposes that are directly related to one of our functions or activities which would be reasonably expected, including our legal duty of care.

Only personnel who are involved with customer care, support and treatment can access customer personal information. Information that is essential for continuing service and EACH's management, funding and quality assurance may be accessed by other appropriate personnel within EACH. For example, some administrative personnel may have access to personal information in the course of their duties. The extent of this access is limited to information that is relevant for them to perform their official duties.

We do not disclose personal information to other organisations or anyone else unless:

- There is consent for the disclosure.
- It would be reasonably expected, or have been told, that information of that kind is usually passed to those individuals, bodies, or agencies.
- It prevents or lessens a serious threat to somebody's life or health.
- It is reasonably necessary for a law enforcement function.
- It is otherwise required or authorised by law.

Some information we collect is used to help plan our services, for reporting purposes to our funding bodies and for quality improvement. This information may also be used for research to help us to provide better overall healthcare for the community. As this information is not personally identifiable, specific consent to this is not required.

For some services, information may be shared to assess or manage family violence risk, or to promote the wellbeing or safety of a child. This information may be shared without the customers consent if there is a serious threat to the customer's or another person's life, health, safety, or welfare. It may also be shared without consent if it is necessary to assess or manage family violence risk to a child, or to promote the wellbeing or safety of a child.

Some of our funding agreements with government require transfer of personal files and information back to the funding body at the conclusion of the contract.

EACH is a national organisation. Personal information may be transmitted to organisations outside the customer's home state. This is only done where there is explicit consent, or where the recipient organisation is subject to similar, binding privacy obligations and it is impracticable for the customer to provide consent, but it is reasonably believed that the customer would give consent.

We do not intend to disclose personal information to overseas recipients.

Organisations that we regularly disclose information to include:

- The Department of Health and the Department of Fairness, Families and Housing (Vic) are organisations to which we may be required to disclose personal information and return files, for example at the conclusion of funding contracts.

- The National Disability Insurance Agency (NDIA). The [National Disability Insurance Scheme Act 2013](#) s55(1) gives the NDIA the power to require production of information that is, among other matters, relevant to the functions of the NDIA.
- Those organisations included in the Family Violence Information Sharing Scheme ([Family Violence Protection Act 2008](#) (Vic)) and Child Information Sharing Scheme ([The Children Legislation Amendment \(Information Sharing\) Act 2018](#) (Vic)).

2.1.6 Data quality

We take steps to ensure that the personal information we collect is accurate, current, and complete. This includes maintaining and updating personal information when we are advised that personal information has changed, and at other times as necessary.

2.1.7 Data security

We take reasonable steps to protect the personal information we hold against loss, unauthorised access, use, modification, or disclosure and against other misuse. These steps may include password protection and encryption of digital information and securing paper files with physical access restrictions.

Access to personal information held on computer systems is controlled and monitored. Only personnel required by their duties to have access to records and information systems are authorised to access such information.

When no longer required, personal information is destroyed in a secure manner in accordance with the law and the requirements of our funding agreements.

2.1.8 Access and correction

Access to personal information is available on request. However, information relating to others or where the information would otherwise be exempt from disclosure by law is not to be given. Proof of identity must be presented to us before personal information is released. Requests are made in writing and addressed to the Privacy & Health Records Coordinator.

If we do not agree to provide access to personal information, the steps to take to seek a review or to appeal our decision (as applicable) are explained.

EACH provide contracted government services and as a result we may receive personal information requests under *Freedom of Information* legislation. This would occur when an individual receiving services at EACH has made a request for access to their personal information directly with the government agency responsible for administering and funding that service. EACH is contractually obliged to comply with these requests.

Requests to correct personal information held by EACH can be made to the Privacy & Health Records Coordinator. Requests are made in writing and must provide evidence to support the requested changes. If we do not agree to make the requested changes to personal information, a statement about the requested changes can be made and attached to the customer file.

2.1.9 Complaints about privacy

If there are concerns about the way we handle personal information, or a complaint relating to privacy matters, please forward details of the complaint to feedbackandcomplaints@each.com.au. The complaint is then referred to the EACH Customer Feedback Coordinator who investigates the matter if this is required.

Privacy complaints at EACH will be handled in line with the EACH Feedback and Complaints procedure.

2.1.10 Privacy breaches

A privacy breach is unauthorised access or disclosure of EACH personnel, customer, or organisational information. A privacy breach may trigger reporting obligations under the [Privacy Act 1988 \(Cth\)](#).

2.2 Information collected online by EACH

2.2.1 Collection

It is our usual practice to collect information about all visitors to our online resources. That information is very limited and only used to identify generic visitor behavioural patterns.

Sometimes we use third party platforms to deliver information. These are sites hosted and managed by organisations other than ourselves. Before deciding if you want to contribute to any third-party site read their privacy policy.

There are several methods and packages that we use to collect visitor behaviours on each of our online platforms. We use Google Analytics on our websites. Information and data collected through Google Analytics is stored by Google on servers in the United States of America, Belgium, and Finland. Customers can opt out of the collection of information via Google Analytics by downloading the Google Analytics Opt-out browser add on.

When you visit any of our online resources, our metric tools may collect the following information about your visit for statistical purposes:

- server address
- top level domain name (for example .com, .gov, .au, .uk etc.)
- the date and time of your visit to the site
- the pages you accessed, and documents downloaded during your visit
- the previous site you visited
- if you've visited our site before
- the type of browser used.

We record this data to maintain our server and improve our services. We do not use this information to identify anyone personally.

2.2.2 Cookies

Most of our online platforms use sessions and cookies. The core functionality on these platforms will be largely unaffected if cookies are disabled in the user's browser but the user may be unable to access some advanced functions.

2.2.3 Data quality

We correct any personal information that we hold on request.

If you are on one of our automated email lists, you may opt out of further contact from us by clicking the 'unsubscribe' link at the bottom of the email.

2.2.4 Data security

There are inherent risks in transmitting information across the internet and we do not have the ability to control the security of information collected and stored on third party platforms. In relation to our own servers, we take all reasonable steps to manage data stored on our servers to ensure data security.

2.2.5 Access and correction

For information about how to access or correct personal information collected on our website see 'Access and correction' (section 2.1.7) in this document.

2.3 Further information

Contact us to obtain further information regarding this privacy policy or to provide any comments.

Telephone 1300 00 EACH (1300 00 3224)
Email privacyofficer@each.com.au
Post 20 Melbourne Street, Ringwood, Victoria 3134

3.0 DEFINITIONS

Customer: EACH is committed to being a customer centric organisation. Our broad definition of customer means we are inclusive of all people who interact or engage with us, either externally or internally. Our customers include consumers, clients, participants, patients, carers, the community, stakeholders, partners, staff, volunteers and members.

Consent: Refers to the agreement of the customer (or authorised representative) to a proposed action. Consent can be expressed or implied and must be current, specific, voluntary and the customer must have the capacity to understand what they are consenting to and its effects.

EACH Personnel: All employees (whether employed full-time, part-time, fixed term or on a casual basis) Board members, volunteers, students, contractors and sub-contractors performing work on behalf of EACH.

Health Information: All information, (personal and health) collected to provide, or in the course of providing, health services

Implied Consent: In situations where we have not yet or are unable to obtain express consent, consent to record and store information a customer has provided may be inferred.

Informed Consent: Ensures that consent is properly obtained, is legal, ethical and a professional requirement on the part of EACH personnel and supports person-centred care.

Personal information means 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.

Sensitive Information: Information or an opinion about an individual's race, ethnic origin, political opinion, beliefs or affiliations sexual preference or criminal record. It also includes health information

4.0 DOCUMENT OWNER

The Privacy & Health Records Coordinator is the subject matter expert and person responsible for this document review.

5.0 REFERENCES AND RELATED DOCUMENTS

- [Data Breach Response Procedure](#)
- [Information Security Policy](#)
- [Information Security Procedure](#)
- [Informed Consent Procedure](#)
- [Collection and Use of Personal and Sensitive Information Procedure](#)
- [Delivering services with trust and respect brochure](#)
- [Health Services Act 1988 \(Vic\)](#)
- [Privacy and Data Protection Act 2014 \(Vic\)](#)
- [My Health Record Act 2012 \(Cth\)](#)
- [Family Violence Protection Act 2008 \(Vic\)](#)
- [The Children Legislation Amendment \(Information Sharing\) Act 2018 \(Vic\)](#)
- [Privacy Act 1988 \(Cth\)](#)
- [Health Records Act 2001 \(Vic\)](#)
- [Health Records and Information Privacy Act 2002 \(NSW\)](#)
- [Information Privacy Act 2009 \(Qld\)](#)
- [Health Records \(Privacy and Access\) Act 1997 \(ACT\)](#)
- [The Children Legislation Amendment \(Information Sharing\) Act 2018 \(Vic\).](#)
- [Family Violence Protection Act 2008 \(Vic\)](#)
- [National Disability Insurance Scheme Act 2013](#)