Privacy, Confidentiality and Information Security Policy

V3 |Last Reviewed: 19/08/2024

Purpose and Scope

This Policy applies to all employees, including management of EnableOT when handling all personal and sensitive information to ensure correct usage, storage and security, also in accordance with law.

Clients, their stakeholders and staff have legislated rights to confidentiality and privacy, and to accessing their own records. It is essential that we protect and uphold these rights, and that we act correctly in those circumstances where the right to confidentiality or privacy may be overridden by other considerations.

Legislative Requirements

Commonwealth Privacy Act 1988:

This Act creates a scheme of National Privacy Principles for the responsible collection and handling of personal information. Organizational practices must ensure that personal information is secure, accurate and only used for the purpose for which it was collected.

NDIS Act 2013 (The Act):

The National Disability Insurance Scheme (NDIS) was developed to enable people with disability to live 'an ordinary life' as others in society do. The associated Act aims to provide for the National Disability Insurance Scheme in Australia, support the independence and social and economic participation of people with disability, provide reasonable and necessary supports, including early intervention supports, for clients in the National Disability Insurance Scheme launch, enable people with disability to exercise choice and control in the pursuit of their goals and the planning and delivery of their supports, facilitate the development of a nationally consistent approach to the access to, and the planning and funding of, supports for people with disability, promote the provision of high quality and innovative supports that enable people with disability to maximise independent lifestyles and full inclusion in the mainstream community, raise community awareness of the issues that affect the social and economic participation of people with disability, and facilitate greater community inclusion of people with disability.

Privacy and Confidentiality

EnableOT collects personal or sensitive information for the purpose of delivering direct services, administering processes associated with service delivery e.g. referrals, meeting any requirements for government funding, monitoring or evaluating the services we provide, to comply with legal obligations or to produce annual reports or for research purposes. The nature and extent of the information collected by EnableOT varies depending on the individual's interaction with us. This information may be collected by EnableOT using in-person interviews, service entry processes, online or electronic communications, questionnaires or over the telephone. A brief summary of how we collect and use a client's private information is written at the end of the **Client Contact Details** form that is forwarded as part of onboarding new clients. This includes an invitation for a person to inquire further if they have questions about how we manage their personal information. This Privacy, Confidentiality and Information Security Policy is then provided to them with a personalised explanation according to the nature of the questions they have, and the best way to ensure comprehension.

As with other key information frequently commonly provided to new clients at the commencement of service delivery, inundating our clients with privacy information upfront is detrimental to crucial therapeutic relationship building as it is experienced as overwhelming. For this reason, EnableOT gives clients a link (sent via our **Welcome to EnableOT SMS**) to a webpage containing the information, but intentionally refrains from discussing any 'privacy' speak unfront, instead engaging immediately in meeting a primary need and forming a connection with the client and their informal supports.

Collection of Personal Information

EnableOT will only collect personal information where it is necessary for EnableOT' functions and activities or is otherwise authorized by law. EnableOT will collect personal information by lawful and fair means and not in an unreasonably intrusive way. EnableOT will only collect sensitive information if the individual provides it voluntarily, consents to EnableOT collecting it, or as otherwise authorized by law.

The personal information EnableOT collects may include:

- Contact details (name, address, email, etc.)
- Personal details (date of birth, gender, income, emergency contacts, etc.)
- Information on personal issues and experiences, areas of interest or relationships
- Family background or supports that clients may have in the community
- Cultural or religious requirements and adjustments that account for these sensitivities
- Health information and/or medical history
- Criminal history
- Credit card or bank account details or NDIS funding details
- IP address of website visitors

Use of Personal Information

Personal information will only be used for the primary purpose(s) for which it was collected and in some cases for related secondary purposes or as set out below. Use of personal information for research purposes is not permitted unless this was the purpose for which the information was collected and the people the information was collected from gave their free, prior and informed consent. Where EnableOT Staff need to use personal information for purposes other than the stated purpose, they must obtain consent where appropriate and necessary.

Exceptions to this include where:

- the use is required to lessen or prevent a serious and imminent threat to an individual's life, health or safety, or to public health and safety;
- EnableOT suspects fraud or unlawful activity;
- the use is necessary to assist a law enforcement agency in its law enforcement functions; or
- the use is required or authorized by law.

Other than in cases of emergency, Sensitive Information may only be used and accessed by EnableOT staff for purposes other than the stated purpose where there is a clear and compelling organizational or other need to do so.

Disclosure of Personal Information to Third Parties

EnableOT staff may only disclose personal information to other persons or entities for the primary purpose(s) for which that personal information was collected. This usually includes when personal information is disclosed to other organizations or professionals working with that client. Examples could include disclosing information to the Department of Human Services, Drug and Alcohol Services or schools, and circumstances where a decision not to disclose the information would prevent us providing the service a client expects us to provide.

Where an EnableOT staff member wishes to disclose personal information for purposes other than these purposes, they must obtain consent where appropriate and necessary.

EnableOT is not required to obtain consent where:

- the disclosure is required to lessen or prevent a serious and imminent threat to an individual's life, health or safety, or to public health and safety;
- EnableOT suspects fraud or unlawful activity;
- the disclosure is necessary to assist a law enforcement agency in its law enforcement functions; or
- the disclosure is required or authorised by law.

Quality, Accuracy, Retention and Destruction of Personal and Other Information

All EnableOT staff must take reasonable steps to ensure that any personal information they collect, use or disclose is complete, accurate and up-to-date. If any EnableOT staff member becomes aware that any personal information EnableOT holds is not accurate, they are required to update and correct the information promptly. Where staff become aware that the personal information EnableOT holds in relation to them changes or is no longer accurate the staff member should provide updated information as soon as practicable. EnableOT is committed to allowing individuals to access and correct personal information about them.

EnableOT may only keep personal information for as long as it is necessary to fulfil organizational needs or legal requirements. If a decision is made by EnableOT to destroy or dispose of documents, this is done in a secure manner using reputable secure shredding services.

Other information (not client-specific) that becomes outdated (such as past versions of templates or policies etc) are removed from the central access point (a page of the EnableOT website that is only accessible to EnableOT team members) and stored indefinitely in Archive Folders on EnableOT Servers. The new versions of superseded documents are then placed at a central access point so that the latest version is always the version available. Staff are informed via **Mattermost**, during supervision sessions and on Team Weekends, that a new version has been uploaded and they are to destroy any former versions they have downloaded. EnableOT practices a system of version tracking to ensure the easy ability to distinguish current versions from their predecessors.

Exceptions to the General Right of Access

EnableOT may decide that it is not appropriate for an individual to access their personal information in circumstances where:

- providing access would pose a serious and imminent threat to the life or health of any individual;
- providing access would have an unreasonable impact upon the privacy of other individuals (this may be relevant where information about other individuals is included on a file);
- the request for access is frivolous or vexatious;
- the information relates to existing or anticipated legal proceedings where the information would not otherwise be discoverable;
- providing access would be unlawful;
- denying access is required by law;
- providing access would prejudice an investigation of possible unlawful activity;
- providing access would prejudice law enforcement; or
- the personal information requested is an employee record and is not health information

If EnableOT refuses a request for access to the personal information, EnableOT will provide reasons why this is the case. In cases where EnableOT does not wish to grant direct access to an individual to the personal information held about the individual, then an agreed intermediary may be used to explain that information to the individual.

Accessing and Amending Records

Individuals may request amendments to their personal file and information collected, used and stored about them. If EnableOT believes it is inappropriate to alter the information, or if amendment may result in harm to self or others, EnableOT will also provide reasons why this is the case and include a statement about the disputed facts regarding the relevant file.

Physical Privacy

When talking to client or their guardians about information of a private or personal nature, staff will:

- Ensure they are the most appropriate staff member to be interviewing or discussing information of a private or personal nature
- Provide options for physically separated spaces such as private offices or interview rooms or at the client's home if requested

- Provide options for private telephone calls to ensure personal information cannot be overheard
- When accompanying a client to a community activity, as much as possible EnableOT's team members attempt to be in the role of an acquaintance rather than clinician, in order to facilitate natural integration of the client into that community group – only disclosing their role as clinical support if absolutely necessary to make client effective participation possible.
- Explain to the individual that they may request a support person or advocate in attendance, especially if there are cultural or religious requirements that have been identified on file, requests for a support person or cultural and religious adjustments will not be unreasonably denied
- Clients or their guardians will have access to any notes from the meeting, during or after the meeting or after the notes are placed on their file in line with the Australian Privacy Principles. A client or guardian may request access to their file through written request and this request will not be unreasonably denied.

Information Security

EnableOT staff must take all reasonable steps to protect and secure personal information and to safeguard personal information from misuse, loss and unauthorized access, modification and disclosure. Security measures will take account of the form in which personal information is stored including in hard copy and digital or electronic formats. Security for personal information will include passwords for IT systems, locked filing cabinets and physical access restrictions. Personal information no longer required to be retained by law will be securely destroyed or de-identified.

EnableOT ensures that safeguards are in place to protect the personal information it administers against loss, interference, unauthorised access or disclosure, modification or other misuse. These safeguards include reasonable physical and technical steps for both electronic and hard copy records. Some of these include, but are not limited to:

- EnableOT will keep any hardcopy client and employee files secure in a locked cabinet, away from public areas, and will make sure only staff who require file access in the course of their expected duties are able to see them
- Positioning electronic equipment so that they cannot be seen or accessed by unauthorized persons, including being aware of telephone conversations that may be overheard by other staff or client stakeholders
- Electronic files will be secured using password protection on all computers and mobile devices, electronic encryption of files stored within the cloud as well as anti-viral software, malware protection and firewalls to restrict unauthorized use through internet security software
- Electronic files will be stored on an EnableOT-located secure server based on a RAID system of storage, with back up to another EnableOT-located server at a different site – to protect against the loss of data by degradation of hard drives, or server damage at one site.
- All clinical staff have synchronising folders on their main work PC, and their clinically-used Smart Devices where they are required to locate client related working documents – so that damage to their PC or other devices does not result in the loss of critical working documents. This folder is deleted, after all EnableOT client data has been transferred to archive, should a clinical team member depart working with EnableOT.
- All formal clinical documentation is to take place in four places:
    1. **Halaxy Platform**:
        - This is a secure Australian-based, Medicare-acceptable, platform, where data integrity can be established.
        - Basic demographic, referral, funding and appointment details are recorded here, to facilitate invoicing.
        - All Internal Audit **Client Reviews (Initial, Ongoing & Final)** are also completed here for audit tracking.
        - EnableOT's Practice Manager is responsible for downloading a copy of EnableOT's entire clinical records from Halaxy on at least a monthly basis.
    2. **EnableOT NextCloud Server:** All other documentation related to client care is stored securely onsite in Cairns (and backed-up to staff-based locations within Queensland), within a Client-specific folder. The folder is shared between staff when working together with a client. Only staff working directly with the client, Enable's Management Team, and Enable's internal Tech Team, have access to a

client's documentation (the Tech Team does not read what is contained in folders, only has access in order to manage staff access).

3. **JotForm Form-Builder Platform:** Used for secure external and internal completion of forms, such as Client Detail forms that we issue to each new client in order to collect required data as an Australian-based Allied Health Practice. Jotform is based in the USA and uses overseas servers, but the data is encrypted and the platform complies with HIPAA (USA Health-cyber-security standard), the EU Standards for health services (even stricter than HIPAA), and Australian-based cyber security for health service requirements. There is no Australian-based form-builder platform with this level of health-data security available currently, which is why EnableOT uses Jotform.
4. **RediCASE Platform:** For any clients referred to us via the Commonwealth-funded Mental Health Stepped-Care Program, through North Qld Primary Health Network (NQPHN), a requirement of the funding is that we also fully document on the secure, Australian-based, RediCASE Platform. Only clients funded under that program are documented here. EnableOT's Practice Manager is responsible for downloading a copy of EnableOT's entire clinical records from RediCASE on at least a monthly basis.

- Mobile Data App functionality is entirely internal to EnableOT. Staff smartphone devices link securely directly to that App's database on EnableOT's server – which is also backed up.
- Traceability of records including attributing author and date to handwritten documents
- Disposing of records securely, when they are no longer required and transferring them to a more appropriate agency in accordance with the Access, Entry, Provision and Exit Policy.
- Refraining from using any Google-based (or other mass data collecting) platform/tool for anything sensitive (eg. Google voice recognition, underpinning all voice recognition apps). They must check with EnableOT technical support to confirm a platform or digital tool is safe from data mining.

Privacy Breaches

All staff must immediately report any breaches or potential breaches of this policy (privacy breaches) via the Mobile Data App: Event of Concern Project. This includes circumstances where they believe any personal information from employee or client related records, files or databases has been lost, misplaced or stolen or where it has been accessed, transmitted or released for an unauthorized purpose. It includes where personal information has been delivered, posted, emailed or faxed to the incorrect address, organization or person. Where staff believe there has been, or they have caused a privacy breach, they should act immediately to contain or minimize the breach including if possible, retrieving or securing information.

EnableOT business owners have primary responsibility for containing and investigating privacy breaches. Any staff member found to have deliberately breached this Policy will be subject to appropriate disciplinary action, which may include dismissal. Where staff have inadvertently or negligently contributed to a privacy breach, they will be subject to appropriate action which may include counselling, increased supervision, additional training, disciplinary or other appropriate action.

It should be considered whether to notify any other parties of the breach. If there has been a breach that may result in the risk of serious harm (reportable incident), then the incident is reportable to the Office of the Australian Information Commissioner. See Guide to handling personal information security breaches (August 2008) published by the Office of the Privacy Commissioner and available from http://www.privacy.gov.au

Additional Considerations

Consent

In some circumstances (for example when a third party such as a parent wants to see client information) EnableOT may need to determine whether the individual can and will provide consent.
There are no specific rules determining when an individual has capacity to provide consent. The Office of the Federal Privacy Commissioner recommends that as a general principle 'a young person is able to give consent when he or she has sufficient understanding and maturity to understand what is being proposed'.

The ability to provide consent will depend on the age of the individual and whether they have an intellectual disability that may prevent them from having enough understanding of what they are consenting to.

Complaints

If an individual has any concerns about the way in which their personal information is being handled, or they believe that there has been an interference with the privacy of personal information held about them, they may contact any EnableOT staff member who will initiate an Event of Concern process.

Complaints will be handled impartially and as promptly as possible in the circumstances. Only those people who are involved in the investigation of the complaint will have access to personal information in relation to the complaint.

Training

Staff will be trained in Privacy, Confidentiality and Information Security Policy via the NDIS mandatory module as well as training recorded on the **Staff Onboarding Checklists**.

Review

This policy will be reviewed when required by changes to legislation or when organization operations require it. Employees and clients will be consulted in relation to any proposed changes. It is recommended that this policy be assessed at 9 monthly internal review alternating with formal auditing processes.