Western Sydney Speech Pathology

www.wssp.com.au
P: (02) 9622 1616 F: (02) 9622 6054
Suite 26 & 27, 15-17 Kildare Road, Blacktown 2148
ABN 32 620 732 890

Privacy And Confidentiality

All patient information is private, and confidentiality of patient information must be always maintained. The rights of every patient are to be respected. All information collected by this practice in providing a health service is deemed to be private and confidential. This practice complies with Federal and State privacy regulations including the Privacy Act 1998, the Australian Privacy Principles (APP's) from Schedule 1 of the Privacy Amendment (Enhancing Privacy Protection) Act 2012 as well as the standards set out in the RACGP Handbook for the Management of Health Information in Private Medical Practice 1st Edition.

Patient Consent

We require your consent to collect and use information about you. This will be done when you join the surgery by completing and signing our new patient form. You can amend your consent at any time, by speaking with our Business Manager or your treating doctor or nurse. Employees of this practice will not discuss or in any way reveal patient conditions or documentation to unauthorised staff, colleagues, other patients, family or friends, whether at the practice or outside it, such as in the home or at social occasions or in social media. This includes patient's accounts, referral letters or other clinical documentation. General Practitioners and staff are aware of confidentiality requirements for all patient encounters and recognise that significant breaches of confidentiality may provide grounds for disciplinary action or dismissal. Every employee of this practice is aware of the privacy policy and has signed a privacy statement as part of their terms and conditions of employment. This privacy statement continues to be binding on employees even after their employment has terminated.

Your Information

We collect personal and health related information for the primary purpose of providing comprehensive, ongoing, holistic Speech Therapy care to individuals and families in accordance with accepted, high standards and requirements. The minimum personal and health details we require to be able to provide you with the best care and therapy include:

- Your full name (As held by Medicare)
- Date of birth
- Residential address and postal address
- Contact phone numbers
- Current Medicare
- Current Health Care Card
- Current medications or treatments used by the patient
- Previous and current medical history, including where clinically relevant a family medical history
- The name of any health service provider or medical specialist to whom the patient is referred,
- Copies of any letters of referrals and copies of any reports back.
- To assist us in providing you with the best possible care you will also be asked for information about:
- If you identify as Aboriginal or Torres Strait Islander

- Lifestyle information such as nutrition, exercise
- Cultural information such as languages spoken and country of origin

Information Use & Disclosure

We may access your health information for:

- Administrative purposes in running our clinical practice.
- Billing purposes, including compliance with Medicare and Health Insurance Commission requirements.
- Disclosure to others involved in your healthcare including treating doctors and specialists outside this medical practice. This may occur though referral to other doctors, or for medical tests and in the reports or results returned to us following referrals.
- Disclosure to other doctors in the practice, locums etc. attached to the practice for the purpose of patient care and teaching.
- For research and quality assurance activities to improve individual and community health care and practice management. Usually information that does not identify you is used but should information that will identify you be required you will be informed and given the opportunity to "opt out" of any involvement.
- For reminder letters which may be sent to you regarding your health care and management.
- For preventative health programs
- Personal information collected by us may be used or disclosed:
- For the purpose the patient was advised of at the time of collection of the information by us;
- As required for delivery of the health service to the patient;
- As required for the ordinary operation of our services (i.e. to refer the patient to a medical specialist or other health service provider); As required under compulsion of law; or
- Where there is a serious and imminent threat to an individual's life, health, or safety; or a serious threat to public health or public safety.

Other than as described in this Policy or permitted under the National Privacy Act, this Practice uses its reasonable endeavours to ensure that identifying health information is not disclosed to any person. Some of this information will be used for directly related reasons such as providing a referral to a specialist, hospital or other health service. We may also use information within the practice for our own quality assurance and education programs, to provide you with reminder letters, to inform you of health related issues or programs which may be of interest and for accounting purposes, including Medicare billing.

Records And Security

Our patient records are maintained in a secure on-site computer system. The information recorded is protected by an individual password system and is accessible only to authorized personnel. Records will be retained for at least 7 years after the last encounter in the case of adults and for children, until they have attained the age of 25 years. Paper based information that is no longer required is destroyed by shredding. All authorized practice doctors and staff have access to your information – if you see different doctors, they all have access to your record unless you specifically request otherwise. At times we write to our patients about health related matters and reminders for follow up appointments. Your name can be removed from such lists if required.

Introduction

This privacy policy is to provide information to you, our patient, about how your personal information (which includes your health information) is collected and used within our practice, and the circumstances in which we may share it with third parties.

Why and when your consent is necessary

When you register as a patient of our practice, you provide consent for our Speech Pathologists and practice staff to access and use your personal information so they can provide you with the best possible healthcare. Only staff who need to see your personal information will have access to it. If we need to use your information for anything else, we will seek additional consent from you to do this.

Why do we collect, use, hold and share your personal information?

Our clinic will need to collect your personal information to provide healthcare services to you. Our main purpose for collecting, holding, using and sharing your personal information is to manage your treatment. We also use it for directly related business activities, such as financial claims and payments, practice audits and accreditation, and business processes (e.g. staff training).

What personal information do we collect?

The information we will collect about you includes your:

- names, date of birth, addresses, contact details.
- medical information including medical history, medications, allergies, adverse events, immunisations, social history, family history.
- Medicare number (where available) for identification and claiming purposes.
- healthcare identifiers & health fund details.

How do we collect your personal information?

- Our practice may collect your personal information in several different ways.
  When you make your first appointment our practice staff will collect your personal and demographic information via your registration. Please see our Consent Form which states how we collect and use your personal information.
- During the course of providing our services, we may collect further personal information. Information can also be collected through electronic transfer of prescriptions (eTP), My Health Record, e.g. via Shared Health Summary, Event Summary.
- We may also collect your personal information when you visit our website, send us an email or SMS, telephone us, make an online appointment or communicate with us using social media.
  In some circumstances personal information may also be collected from other sources. Often this is because it is not practical or reasonable to collect it from you directly. This may include information from:
    a. your guardian or responsible person
    b. other involved healthcare providers, such as specialists, allied health professionals, hospitals, community health services and pathology and diagnostic imaging services
    c. your health fund, NDIS or Medicare.

When, why and with whom do we share your personal information?

We sometimes share your personal information:

- with third parties who work with our practice for business purposes, such as accreditation agencies or information technology providers – these third parties are required to comply with APPs and this policy.
- with other healthcare providers
- when it is required or authorised by law (e.g. court subpoenas)
- when it is necessary to lessen or prevent a serious threat to a patient's life, health or safety or public
- health or safety, or it is impractical to obtain the patient's consent
- to assist in locating a missing person
- to establish, exercise or defend an equitable claim
- for the purpose of confidential dispute resolution process
- when there is a statutory requirement to share certain personal information (e.g. some diseases require mandatory notification)
- during the course of providing medical services
- Only people who need to access your information will be able to do so. Other than in the course of providing medical services or as otherwise described in this policy, our practice will not share personal information with any third party without your consent.
- We will not share your personal information with anyone outside Australia (unless under exceptional circumstances that are permitted by law) without your consent.

Our practice will not use your personal information for marketing any of our goods or services directly to you without your express consent. If you do consent, you may opt out of direct marketing at any time by notifying our practice in writing.

How do we store and protect your personal information?

Your personal information may be stored at our practice in various forms.
e.g. as paper records, electronic records, visual records (videos and photos), audio recordings.
Our practice stores all personal information securely.
Personal information is stored securely e.g. electronic format, in protected information systems or in hard copy format in a secured environment. All electronic communication is via encrypted data and contains multiple password layers. Onsite records are stored in secure cabinets including confidentiality agreements for staff and contractors.

How can you access and correct your personal information at our practice?

You have the right to request access to, and correction of, your personal information.
Our practice acknowledges patients may request access to their medical records. We require you to put this request in writing, our receptionist can provide you with a personal detail update form to change your personal information and will endeavour to update your record on the day of your visit.

How can you lodge a privacy-related complaint, and how will the complaint be handled at our practice?

We take all complaints and concerns very seriously, especially those regarding privacy and consent. You should express any privacy concerns you may have in writing. We will then attempt to resolve it in accordance with our resolution procedure.

Please contact Celine Pascual regarding any privacy related concerns, she can be contacted in writing or in person at Western Sydney Speech Pathology Unit 27, 15-17 Kildare Road, Blacktown 2761 or phone 02) 9622 1616.

You should expect an acknowledgment from the practice within 48 hours specifying the expected turnaround time for our response. You will receive a response to any and all identifiable feedback.

You may also contact the OAIC. Generally, the OAIC will require you to give them time to respond before they will investigate. For further information visit www.oaic.gov.au or call the OAIC on 1300 363 992

Policy review statement

This privacy policy will be reviewed regularly to ensure it is in accordance with any changes that may occur. Updates will be notified by signage in our waiting room, updates to our privacy brochures and via our website.

You may also receive a text regarding changes to our policies if you have nominated to be contacted this way.

Remember you may update your preferred method of contact at any time with our friendly staff.

What if I am with NDIS?

Our policy is to respect and protect the privacy of all people connected with the NDIA, including participants, providers, employees, contractors and community partners. This Privacy Policy tells you the kinds of personal information we, and others for us, collect and hold, how and why we collect and hold that information and how we use it. It also tells you how you can access and amend your personal information and how you may make a complaint if you think that we have breached our privacy obligations.

Personal information is information or an opinion about an individual whose identity is reasonably identifiable. Examples of personal information include a person's name, address, date of birth and details about their health or disabilities.

Privacy laws do not apply to the information of corporate entities, such as providers or community partners. However, the personal information of individuals connected with those entities (such as employees) will be protected by privacy laws.

In dealing with personal information, we abide by the obligations imposed on us under federal law, including the Privacy Act 1988 (Cth) Privacy Actand the National Disability Insurance Scheme Act 2013 (Cth) (NDIS Act).

The Privacy Act authorises our collection of personal information where this is required to facilitate access to the NDIS and perform our other functions.

We are also bound by confidentiality and secrecy provisions in the National Disability Insurance Scheme Act 2013 (Cth) (NDIS Act). These provisions limit how we collect and use personal information and when and to whom information can be disclosed.

What kinds of personal information does the NDIA collect and hold?

We collect and hold information which is reasonably necessary for us to carry out our role. The kinds of information we collect and hold includes (but is not limited to) personal information about participants and other users of our services, and about our employees, contractors and providers. Examples of personal information that we may collect includes:

- name, contact details date of birth and age
- gender, details about participants' physical or mental health, including disabilities
- information about participants' support requirements
- details of guardians and nominees, including names, addresses and contact details
- Centrelink Customer Reference Number (CRN)
- details of feedback or complaints about services provided by us

- bank account details
- employee records.

We may also collect some 'health information' as defined under the Privacy Act, such as information about your health or disability, doctors you have seen or health services you have received. Information about an individual that is or was held by the NDIA is considered 'protected information' for the purposes of the NDIS Act.

You can choose to deal with us anonymously, in which case your personal information is not subject to privacy laws. However, if a person becomes, or applies to become, a participant in the NDIS or a registered provider of supports, it is impractical to deal with that person on an anonymous basis and in this case we may not be able to assist you if you seek to deal with us anonymously.

How will the NDIA collect and hold personal information?

We often collect personal information from people directly or from people who are authorised to represent them. While you do not have to provide us with all information requested, not providing this information to us may mean that:

- we may not be able to decide whether you can become a participant;
- decisions may be delayed while we seek further information; and
- we may not be able to approve your plan and the supports funded through the NDIS.

We sometimes collect personal information from a third party if you have consented, been told of this practice, or would reasonably expect us to collect the information in this way. An example of this is collecting information from a healthcare service, such as a residential care facility, which is managing a participant's care.

We, or contracted service providers acting on our behalf, may also collect personal information from third party disability support providers, state and territory governments and other Commonwealth government entities (for example, Services Australia (formerly the Department of Human Services)) where this collection is authorised under law.

Federal law allows us to require the provision of information in certain circumstances. We do this in order to perform our functions, including facilitating the NDIS. The information collected is usually about participants, prospective participants, registered providers or persons with a disability who may wish to access the NDIS and is collected from other government bodies, registered providers of NDIS supports or anyone else who may hold relevant information.

Contracted service providers that may collect personal information on our behalf and access your personal information on our record management systems include:

our community partners; and

other parties contracted to collect information, such as the Services Australia.

We, or entities acting on our behalf, (such as community partners) may contact you by phone, for example, to facilitate your access to the NDIS. In the event we do contact you, we will ask for certain personal information over the phone, but will only request this information once we have explained the purpose for asking for this information and once we have your consent to proceed.

Your personal information may also be collected if and when you communicate with us electronically as described, through the mail or in person. In some cases, we may record your telephone interactions with us.

How do we use and disclose personal information?

We collect, hold, use and disclose personal information for the purpose of providing services, including implementing the NDIS, conducting our operations, communicating with participants and health service providers, conducting research and evaluation on the NDIS, and complying with our legal obligations. For example, our activities in implementing the NDIS may involve conducting an

assessment of an individual's disability in order to determine reasonable and necessary supports, and managing that individual's support payments.
All our personnel (including staff and contractors), board members and community partners are issued with NDIA email addresses. When we need to use personal information for our business purposes, we will limit this use to only those NDIA personnel, board members or community partners who need to know that information. Where business use requires us to email personal information internally to NDIA personnel, board members or community partners, we will use NDIA email addresses to send that information.
If we need to disclose personal information outside the NDIA, we will de-identify the information prior to disclosure, wherever it is practicable to do so. We will not normally disclose a person's personal information to anyone outside the NDIA except where we refer participants to external providers of in-kind supports under an approved NDIS plan; where that person consents; or where the disclosure is authorised or required under law. In such circumstances, we will use an NDIA email address to disclose any personal information if it is sent by email.
Some examples of when we may disclose personal information include:
in delivering the NDIS and our other functions (for example, quality assurance purposes, training and purposes related to improving our services);

referrals to external providers of supports for NDIS participants, or sharing information with support coordinators where this is required for services included in an approved NDIS plan;

this is required or authorised by law, including under the NDIS Act;

it will prevent or lessen a serious and imminent threat to someone's life or health or a threat to public health or safety;

it is a necessary part of an internal investigation following a complaint; or

we engage a contractor to provide some NDIS services and the contractor needs personal information of certain participants, providers, carers or other persons in order to perform that service for us.

We rely on contracted service providers, such as community partners and Services Australia, to undertake certain roles on our behalf. These third parties have access to our records and may use those records in order to facilitate your access to the NDIS or to implement your NDIS plan. When we use third parties, such as community partners and other contractors, to perform certain functions, the third parties are contractually required to work in accordance with the Privacy Act and the NDIS Act, and to access and store all personal information using our IT systems, not their own. The contractor is also required to treat personal information they may see or handle with care and confidentiality. Because we retain control over all personal information, the mere use of that personal information by contracted service providers as required by their role is considered a lawful use by the Agency and does not require your consent.

If you apply to become a participant in the NDIS, you will be asked to provide your consent for us to share your personal information with third parties, such as medical practitioners, accommodation facilities, support coordinators and other government entities. This is required as part of assessing whether you meet the access requirements for the NDIS and to implement your plan, if you do become a participant.

We make a record of some phone calls to help us in ensuring that the service we provide meets the highest standards.

We may use your information to seek feedback from you regarding your level of satisfaction with our services.

Users of the NDIA computer system may at times be able to see a person's name (if the person is a participant, provider of supports, nominee or other person known to the NDIA) when performing duties either as an NDIA employee or on behalf of the NDIA, but are only permitted to record, use or disclose that information if it is directly related to performing those duties.

A state or territory government official may also have access to personal information as part of the intergovernmental arrangements.

We will not sell or rent your information to anyone.

We will, on occasion, disclose personal information to overseas recipients. The situations in which we may transfer personal information overseas include:

the provision of personal information to overseas consultants (where consent has been given for this or we are otherwise legally able to provide this information)

the provision of personal information to recipients using a web-based email account where data is stored on an overseas server, and

the provision of personal information to foreign governments and law enforcement agencies (in limited circumstances and where authorised by law).

It is not practicable to list every country to which we may provide personal information as this will vary depending on the circumstances.

However, you may contact us (using the contact details set out at Part E of this Policy) to find out which countries, if any, your information has been given to.

We always liaise with a participant directly, unless they have a nominee appointed, or they request us to liaise with an authorised representative. In the case of child participants, we liaise with their child representatives (who are usually their parents, or legal guardians), , rather than with them directly.

We may also use personal information of participants, providers and community partners to ensure the integrity of the NDIS, which includes identifying and responding to any fraudulent activities or misuse of NDIS funds.

What happens if we have a data breach?

Policy

Data Breaches must be reported to the Director (Celine Lowe Pascual) as soon as practicable.

A data breach that alleges Deliberate Misuse, Unauthorised Access or Inappropriate Access to personal information by a WSSP team Member may be grounds for misconduct/serious misconduct and may result in disciplinary action.

Unauthorised Access or Inappropriate Access to WSSP personal information, attained from the result of system testing (i.e. checking permissions are working) of system security controls is not considered a Policy Breach, providing that system testing is sanctioned by the Director.

Procedure

1. **Suspected data or privacy breach**
    1. Access to personal information is granted to staff only where this is necessary for work purposes and staff must only access personal information if there is a work related reason for this. Personal information must be protected against loss, unauthorised access or modification, disclosure or misuse.
    2. A suspected data breach is considered to be any event which may have involved Unauthorised Access, Unauthorised Disclosure or Loss of Data involving personal.
2. **Reporting a suspected data breach**
    1. If a team member becomes aware of a suspected data breach, they are to contact the Director as soon as possible with as much information as is available via email: celine@wssp.com.au
    2. The information to be provided includes:
        i. the time and date the suspected data breach was discovered,
        ii. the type of personal information involved,
        iii. the cause and extent of the breach,
        iv. the context of the affected information and the breach, and
        v. the actions undertaken to contain the breach (see clause 5).
    3. WSSP only has thirty (30) days from becoming aware of the breach, to carry out a reasonable and expeditious assessment as to whether there are reasonable grounds to believe that the data breach has been an eligible data breach.
3. **Notification requirements of eligible data breaches**
    1. An eligible data breach arises when the following three criteria are satisfied:
        i. there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that WSSP holds;
        ii. this is likely to result in serious harm to one or more individuals; and
        iii. WSSP has not been able to prevent the likely risk of serious harm with remedial action.
    2. Whether a data breach is likely to result in serious harm requires an objective assessment by the Director based on information immediately available or following reasonable inquiries or an assessment of the data breach. The potential kinds of harms that may follow a data breach include:
        i. identity theft,
        ii. significant financial loss by the individual,
        iii. threats to an individual's physical safety,
        iv. loss of business or employment opportunities,

v. humiliation, damage to reputation or relationships, and/or

vi. workplace or social bullying or marginalisation.

3. The likelihood of a particular harm occurring, as well as the anticipated consequences for individuals whose personal information is involved in the data breach if the harm materialises, are relevant considerations.

4. If WSSP acts quickly to remediate a data breach, and as a result of this action the data breach is not likely to result in serious harm, there is no requirement to notify any individuals or the Australian Information Commissioner. There are also exceptions to notifying in certain circumstances.

5. If personal information is lost in circumstances where subsequent unauthorised access to or disclosure of the information is unlikely, there is no eligible data breach. For example, if the personal information is remotely deleted before an unauthorised person could access the information, or if the information is encrypted to a high standard making unauthorised access or disclosure unlikely, then there is no eligible data breach.

4. **Once a breach is declared eligible**

    1. If a data breach is declared eligible by the Director it will be logged into the incident register.

    2. WSSP is required to prepare a statement and provide a copy to the Office of the Australian Information Commissioner (OAIC). The OAIC's online form is to be used for this process. The form includes WSSP's name and contact details, a description of the Eligible Data Breach, the kind or kinds of information involved, and what steps WSSP recommends to individuals at risk of serious harm, in response to the eligible data breach.

5. **Data Breach Response Plan**

    1. WSSP's Data Breach Response Plan comprises four steps (consistent with the OAIC guide to managing data breaches in accordance with the Privacy Act 1988 (Cth)):

Step 1: Contain the data breach to prevent any further compromise of personal information.

Step 2: Assess the data breach by gathering the facts and evaluating the risks, including potential harm to affected individuals and, where possible, taking action to remediate any risk of harm.

Step 3: Notify individuals and the Commissioner if required. If the breach is an 'eligible data breach' under the NDB scheme, it may be mandatory for JCU to notify.

Step 4: Review the incident and consider what actions can be taken to prevent future breaches.

Step 1 - Contain	Once a data breach is suspected immediate action must be taken to limit the breach. For example, stop the unauthorised practice, recover the records, or shut down the system that was breached. If it is not practical to shut down the system, or if it would result in loss of evidence, then revoke or change computer access privileges or address weaknesses in physical or electronic security. To identify strategies to contain a data breach consider: ▪ How did the data breach occur? ▪ Is the personal information still being shared, disclosed, or lost without authorisation? ▪ Who has access to the personal information? ▪ What can be done to secure the information , or stop the unauthorised access or disclosure, and reduce the risk of harm to affected individuals? Notify the Director During this preliminary stage, be careful not to destroy evidence that may be valuable in identifying the cause of the breach, or that would enable the entity to address all risks posed to affected individuals or the entity.
Step 2 - Assess	An assessment of the data breach will identify the risks posed by a data breach and how these risks can be addressed and must be conducted as expeditiously as possible by the Director based on the information available. The aim is to understand the risk of harm to affected individuals, and identify and take all appropriate steps to limit the impact of a data breach. Considerations in this assessment include: ▪ the type or types of personal information involved in the data breach; ▪ the circumstances of the data breach, including its cause and extent; and ▪ the nature of the harm to affected individuals, and if this harm can be removed through remedial action. Remedial action to reduce any potential harm to individuals should be taken (such as recovering lost information before it is accessed). This might also take place during Step 1: Contain. The Director is to determine whether the data breach is an eligible breach under the Notifiable Data Breach (NBD) scheme. This assessment is to occur within 30 days and determined in accordance with the criteria for assessing a data breach, including the risk of harm and remedial action at sect 3. If it is an Eligible Data Breach, the Director will notify the team.
Step 3 - Notify	Notification to affected individuals may be considered for data breaches but must be undertaken for eligible data breaches under the NDB Scheme. Notification can be an important mitigation strategy that has the potential to benefit both WSSP and the individuals affected by a data breach. However, notifying individuals can cause undue stress or harm. For example, notifying individuals about a data breach that poses very little or no risk of harm can cause unnecessary anxiety. It can also de-sensitise individuals so that they don't take a notification seriously, even when there is a real risk

	of serious harm. Each incident needs to be considered on a case-by-case basis to determine whether breach notification is required. In considering to notify individuals who may be impacted by a data breach the following should be considered: ▪ what information is provided in the notification and how this will be provided; ▪ who is responsible for notifying individuals and creating the notification; ▪ who else other than affected individuals (and the Commissioner if the notification obligations of the NDB scheme apply) should be notified; ▪ where a law enforcement agency is investigating the breach, it may be appropriate to consult the investigating agency before making details of the breach public; and ▪ whether the incident triggers reporting obligations to other entities (eg TEQSA or the Australian Taxation Office). Effective data breach response is about reducing or removing harm to affected individuals, while protecting the interests of WSSP. Notification has the practical benefit of providing individuals with the opportunity to take steps to protect their personal information following a data breach, such as by changing account passwords or being alert to possible scams resulting from the breach. Individuals who have been affected by a data breach must be dealt with sensitivity and compassion, in order not to exacerbate or cause further harm. Notification may also serve to demonstrate that privacy protection is taken seriously. The decision to notify will be made by the Director in consultation with our team as necessary. If it is an eligible data breach, notification options include: ▪ Option 1 – Notify all individuals whose personal information was part of the eligible data breach and would be used when WSSP cannot reasonably assess which particular individuals are at risk of serious harm from an eligible data breach that involves personal information about many people, but serious harm is likely for one or more of the individuals. ▪ Option 2 — Notify only those individuals at risk of serious harm. ▪ Option 3 — Publish notification If neither option 1 or 2 above are practicable, for example, if the entity does not have up-to-date contact details for individuals, this may include providing a copy of the statement on the website and take reasonable steps to publicise the statement.
Step 4 - Review	A Lessons Learned Report will be completed on an eligible data breach incident to improve personal information handling practices. This might involve: ▪ a security review including a root cause analysis of the data breach; ▪ a prevention plan to prevent similar incidents in future; ▪ audits to ensure the prevention plan is implemented;

	▪ a review of policies and procedures and changes to reflect the lessons learned from the review; ▪ changes to staff selection and training practices; and ▪ a review of service delivery partners that were involved in the breach. The intent of the Lessons Learned Report is to strengthen WSSP's personal information security and handling practices, and to reduce the chance of reoccurrence. A data breach should be considered alongside any similar breaches that have occurred in the past, which could indicate a systemic issue with policies or procedures. If any updates are made following a review, staff will be notified in any changes to relevant policies and procedures to ensure a quick response to a data breach.

Privacy Act

The Australian Privacy Principles (APP's) from Schedule 1 of the Privacy Amendment (Enhancing Privacy Protection) Act 2012 cover the private health sector throughout Australia. The Privacy Act requires our practice to abide by the 13 Australian Privacy Principles (APPs):

Australian Privacy Principle 1—open and transparent management of personal information

Australian Privacy Principle 2—anonymity and pseudonymity

Australian Privacy Principle 3—collection of solicited personal information

Australian Privacy Principle 4—dealing with unsolicited personal information

Australian Privacy Principle 5 – notification of the collection of personal information

Australian Privacy Principle 6 – use or disclosure of personal information

Australian Privacy Principle 7 – direct marketing

Australian Privacy Principle 8 – cross-border disclosure or personal information

Australian Privacy Principle 9 – adoption, use or disclosure of government related Identifiers

Australian Privacy Principle – 10 quality of personal information

Australian Privacy Principle – 11 security of personal information

Australian Privacy Principle – 12 access to personal information

Australian Privacy Amendment 12 - (Notifiable Data Breaches) Act 2017

Australian Privacy Principle – 13 correction of personal information