PRIVACY AND CONFIDENTIALITY MANUAL

If this information would be more accessible to you in another format, please let us know.

We work on the land of the Dharug people and pay our respects to Elders past and present. We acknowledge that sovereignty was never ceded.

Legal name	Whole Family Health Pty Ltd
Business/trading name	Whole Family Health
ABN	78 614 504 111
ACN	614 504 111
Head office	382 Great Western Highway, ST MARYS, NSW 2760
Phone	(02) 9833 3363
Email	theteam@wholefamilyhealth.com.au
Website	www.wholefamilyhealth.com.au
Person responsible	Geordan Nicholson
Version	1
Date	10 May 2023

TABLE OF CONTENTS

Privacy and Confidentiality Manual 3
1 Definitions & Key Concepts 3
1.1 Consent & Capacity 3
1.1.1 Consent 4
1.1.2 Capacity to Consent 4
1.1.3 Authorised Representatives 5
2 Scope & Responsibilities 6
2.1 Responsibilities 6
2.1.1 The Directors 6
2.1.2 Internal Auditors 7
2.1.3 Managers and Supervisors 7
3 Policy 8
4 Privacy & Confidentiality Procedures 9
4.1 What We Collect 9
4.1.1 Health Information 9
4.2 Collection and Use of Information 10
4.2.1 Information on Collection of Health Information 11
4.3 Disclosure of Information to Third Parties 11
4.3.1 Health Information 12
4.4 Access To and Correction Of Information 13
4.4.1 Access 13
4.4.2 Correction 13
4.4.3 Who Else Can Access Information 14
4.5 Storage and Destruction of Information 14
4.6 Complaints 14
4.7 Employee Information 15
4.7.1 Disclosure of Staff Information 15
4.8 Monitoring and Review 17
5 Privacy Data Breach Procedures 18
5.1 Assess & Determine The Potential Impact 18
5.2 Minor Breach 18
5.3 Moderate to Major Breach 19
6 Revision History 20
6.1 4 May 2023 – v0.1 20
6.2 7 May 2023 – v0.2 20
6.3 10 May 2023 – v1.0 20

PRIVACY AND CONFIDENTIALITY MANUAL

The purpose of this document is to ensure Whole Family Health upholds the privacy and confidentiality of all people including participants, carers and staff. All members of staff must abide by this document.

1 Definitions & Key Concepts

APPs – refers to the 'Australian Privacy Principles' as contained in the *Privacy Act 1988* (Cth) schedule 1.

Disclose – in regard to information, refers to giving a copy of the information to a third party or allowing a third party to access the information.

Health information – any personal information collected to provide, or in providing, a health service (including a disability service) to an individual, or any personal information about:

1) The health or disability (at any time) of an individual;
2) An individual's expressed wishes about the future provision of health services to themselves; or
3) A health service provided, or to be provided, to an individual.

Health service – includes counselling, occupational therapy, physiotherapy, psychology, speech therapy, music therapy and feeding therapy services, and auxiliary services, goods, advice, care or treatment provided in relation to those services or as a consequence of those services.

HPPs – refers to the 'Health Privacy Principles' as contained in the *Health Records and Information Privacy Act 2002* (NSW) schedule 1.

HRIP Act – the *Health Records and Information Privacy Act 2002* (NSW).

Individual – references to an 'individual' or 'you' include references to an authorised representative or responsible person of the individual, where the individual is incapable by reason of age, injury, illness, physical or mental impairment of giving or communicating consent to the use of information, or of understanding the nature and effect of any relevant actions.

Personal information – any information or opinion(s) about an identified (or reasonably identifiable) individual, whether or not the information or opinion is true and whether or not the information or opinion is recorded in a material form.

Sensitive information – personal information about an individual's: racial or ethnic origin, political opinions or associations, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association or union, sexual orientation or practices, criminal record, health information or biometric information.

Use – in regard to information, refers to the communication or handling of information within Whole Family Health, between our staff or directly related entities.

1.1 Consent & Capacity

Consent and a person's capacity to consent is an important part of the management of health information and the provision of health services. **Consent** refers to permission for something to happen or an agreement to do something. **Capacity to consent** refers to someone's ability to consent or make important decisions properly and legally. A person cannot consent or make decisions if they don't have the capacity to do so.

There are several situations where we need consent during the management of a person's information. These situations are detailed throughout this document and generally include most uses of sensitive or health information, and uses of personal information that would be against the APPs without the individual's consent. We can only collect sensitive and health information from a person who has consented to the information being collected, unless a lawful exception applies.

We also require consent from a person prior to us sending them any form of electronic marketing or promotional material, and must provide them with an 'unsubscribe' option on any of that material.

1.1.1 Consent

There are several factors involved in consent. Without these factors, consent is invalid.

- Consent should be **informed**. That means that whoever is seeking consent must make reasonable effects to ensure that the person concerned has all the information they need to understand what they are consenting to, why they might want or need it, and what the reasonably foreseeable consequences of both consenting and withholding consent may be.
- Consent is only valid where it is given **voluntarily**. This means that consent is invalid if it's given by someone because of coercion, pressure, or intimidation. A person should have adequate time to make a decision.
- Consent must be **current.** This means that consent cannot be assumed to last forever and (considering the circumstances) consent should be re-sought after a reasonable period of time, or when a reasonable person would assume that the consent would be invalid due to time.
- Consent needs to be **reasonably specific**. This means that blanket or excessively broad consent does not cover all situations. The level of specificity depends on the circumstances, including how sensitive the information may be.
- For a person to provide consent, they must have the **capacity to consent**. This is further discussed below.

Consent can be:

- **Express** – either in writing, verbally, with assistive technology or sign language.
- **Implied** – where consent can be reasonably assumed from the conduct or actions of the person, however there is NOT implied consent for the sole reason that 'if the person knew about the benefits of the thing, they would consent to it', as a person's choice must be upheld at all times.

1.1.2 Capacity to Consent

A person should be assumed to have the capacity to make their own decisions and give their own consent to the management of their information unless there is reasonable evidence to indicate otherwise.

A person cannot give consent or make decisions about privacy or their health if they:

- Cannot understand the general nature and effect of the matter that they are being asked to decide on, or
- Cannot legitimately communicate their intentions about that matter. However, communication does not have to be verbal for it to be valid and all attempts to assist with translation or assistive technology are the responsibility of the health care provider.

A person's incapacity may be due to age, injury, illness, or physical or mental impairment, and may be permanent or temporary.

Just because a person is below the age of 18, they are not necessarily considered incapable of consenting to the disclosure or use of their health information. Generally, people above the age of 16 should not be considered incapable of consenting purely due to their age, however a person or child of any age who is individually determined by a staff member to be capable of consenting or withholding consent must have those wishes upheld.

For information about consent and assent regarding any procedures, please see the Incident Management Policy and Procedure and the Service Delivery and Participation Policy and Procedure.

1.1.3 Authorised Representatives

When a person does not have the capacity to consent, an authorised representative is able to legally make decisions relating to the privacy of that person's health information.

However, if the person *does* have the capacity to consent, the consent and authorisation of the person must be provided before the authorised representative is allowed to do what would normally only be allowed by the person themselves in relation to their health information.

The authorised representative of a person is anyone who is:

- Someone with an 'enduring power of attorney' for the person
- An enduring guardian under the meaning of the *Guardianship Act 1987* (NSW)
- If the person is a child, their parent or guardian
- The person highest up on the following hierarchy:
    1. Their enduring guardian
    2. A spouse (including a de facto spouse) with whom the person continues to have a close relationship with
    3. Someone who cares for the person on a regular basis not for benefit such as payment
    4. A close friend or relative.

If a child has divorced or separated parents, 'parental responsibility' and hence the ability to be an authorised representative of the child is generally given independently to both parents, unless there is a court order in place which states otherwise. A copy of the relevant court order must be kept on the child's file.

An authorised representative does not necessarily have the right to access any and all of a person's health information, particularly if the person has the capacity to consent.

2 Scope & Responsibilities

This document applies to all personal information about any individual. It provides an overview of the responsibilities that Whole Family Health and its staff have regarding personal, sensitive and health information, as well as employee records. This document also details the legal rights that employees and clients and their representatives have in regard to their personal, health and/or employee information.

This document covers 'personal information' that isn't related to an individual's health, as well as two subsets of personal information: 'health information' that's collected to provide our disability services to a person, or is otherwise about their health or health wishes; and 'sensitive information' which includes health information and many types of information a person might consider sensitive, as is described in Part 1 "Definitions & Key Concepts", above.

It's essential that all staff are informed of their individual rights and responsibilities in regard to information privacy and confidentiality. The privacy and dignity of individuals is put at stake if staff ever act irresponsibly with information, and as such staff should take important everyday measures to protect everyone's privacy.

2.1 Responsibilities

All staff including but not limited to allied health professionals, assistants, administrative staff, management, volunteers, students, and contractors/sub-contractors are:

- Individually responsible for ensuring they implement and comply with the HRIP Act, the APPs, this document, and any confidentiality or privacy clause(s) contained in their contract.
- Joint responsibility for actioning and reporting any potential or actual breaches, risks or other issues that may occur in relation to health and personal information.
- Responsible for ensuring that their use of personal information to contact people does not breach the *Spam Act 2003* (Cth).
- Ensure that any questions about privacy are answered adequately or directed to the appropriate person.

2.1.1 The Directors

The Managing Director has the following key obligations:

- Ensure all staff members are aware of their requirements under this document.
- Ensure all staff members are adequately trained in privacy management that is specific to their role.
- Designate a member of staff to whom questions and requests for guidance on information privacy can be directed, and who should support staff in meeting their requirements under this document, and privacy legislation overall.
- Ensure all stakeholders have access to the information in this document.
- Ensure that this document is kept up-to-date with relevant legislation and practices, namely the *Health Records and Information Privacy Act 2002* (NSW) and the *Privacy Act 1988* (Cth).

- Ensure that any Whole Family Health publication meets any relevant privacy requirements.
- Ensure that any Whole Family Health website(s) has a privacy statement or policy in line with APP 1.
- Ensure that employee records are safeguarded and managed in accordance with this document and the *Fair Work Act 2009* (Cth).
- Ensure that all staff contracts address staff requirements of confidentiality and privacy.
- Manage data/privacy breaches.
- Ensure that the use of personal information to contact people does not breach the *Spam Act 2003* (Cth).
- Ensure that intake forms for human clients contain the information contained in section 4.2.1 'Information on Collection of Health Information'.

The Directors and IT personnel have the following key obligations:

- Ensure that any cloud storage software utilised by Whole Family Health adequately secures information stored against reasonable risk.
- Protect against the compromise of passwords to work accounts which hold/access private and/or confidential information.
- Provide guidance and/or rules to inform/govern staff in their use of work associated accounts to assist in the security of their account and the information that the account has access to, e.g., by providing password rules or activating two-factor authentication.

Staff awareness of privacy issues and responsibilities should be promoted in an ongoing and preventative manner.

2.1.2 Internal Auditors

Internal Auditors are responsible for assisting the Directors in meeting their responsibilities, as well as:

- Acting as a point of contact for staff and the public for matters related to privacy
- Ensuring privacy complaints are processed correctly
- Ensuring non-typical requests for access to information are dealt with in accordance with legislation and this document
- Ensuring that employee records are managed in accordance with this document
- Assist in the management of data breaches.

2.1.3 Managers and Supervisors

Managers, supervisors and team leaders are responsible for:

- Providing leadership and direction to ensure that this document is effectively implemented through the conduct of the team/employees they are responsible for
- Monitor the quality and effectiveness of the management or use of health information and take the appropriate action to address any shortcomings or risks.

3 POLICY

Whole Family Health is committed to keeping the personal information of all stakeholders secure and private. This includes potential and actual clients and their families, website users, staff, management and representatives of other agencies, no matter when our relationship with them occurred.

We will ensure that each participant consents to the collection of their personal information and understands the circumstances in which we may disclose this information to others. We will ensure that this Privacy and Confidentiality Manual is accessible to all stakeholders, and we will provide alternative forms of communicating this Manual to people who request it. We will ensure that we provide adequate assistance to anyone who wishes to exercise a right that they have in relation to their privacy.

As a Registered NDIS provider, we are subject to the NDIA's rules and regulations, including the *NDIS Code of Conduct* and the *NDIS Practice Standards*. We also adhere to the *Spam Act 2003* (Cth) which means we will not send electronic marketing messages without consent.

All personal information (including health information) is managed in accordance with the *Privacy Act 1988* (Cth) and the 13 Australian Privacy Principles ('**APPs**') provided within schedule 1 to that Act. We will only collect personal information in accordance with our Privacy Procedures (below).

All health information is collected and managed in accordance with the *Health Records and Information Privacy Act 2002* (NSW) (the '**HRIP Act**') which details 15 Health Privacy Principles ('**HPPs**').

Employee records which are directly related to their employment are managed in accordance with the *Fair Work Act 2009* (Cth), however employee's medical records and other sensitive information is still managed under the APPs. We elect to follow the APPs in relation to employee records.

Staff must be provided with enough information and training to uphold their requirements under this document. Any staff member with concerns, questions or who needs additional specific guidance should direct their questions to the person responsible for this document.

We do not have any control over external websites which we may provide links to and are not responsible for the protection and privacy of any information which is provided whilst visiting external sites. Those websites are not governed by this Privacy and Confidentiality Manual.

4 Privacy & Confidentiality Procedures

4.1 What We Collect

Through your use of our website, services, and products, we collect information about you which may include:

- Your name;
- Your contact details, including your email address, mailing address, street address and your telephone number;
- Your age and your date of birth;
- Your billing and payment information;
- Your demographic information, such as your postcode;
- Your preferences and/or your opinions;
- Information you provide to us through customer surveys, such as your satisfaction with our services;
- Details of products and services we have provided to you or that you've enquired about;
- Your browser session and geo-location data, including statistics such as your page views or searches and your browsing behaviours;
- Information about your access to, use of, and communication with our website, including through the use of Internet Cookies;
- Any other personal information which we request from you, or which is provided to us by third parties.

If you're seeking employment with us, we may also collect candidate information from you.

4.1.1 Health Information

If you access, or enquire about, our health services, we may collect sensitive health information about you in order to record, maintain or improve your health, to diagnose a disability or illness, or to treat an actual or suspected disability or illness.

We can only collect your health information where it is necessary for us in order to provide our services to you, and we can only collect it from you unless it's unreasonable or impractical to do so. The health information we may collect includes:

- Any information or opinions about your physical or mental health or disability, both now and at any other time;
- Information or opinions about your wishes or preferences regarding your health and treatment of your health;
- Information or opinions about health services which are or may be provided to you.
- Information to do with your funding of health services;
- Family history;
- Appointment and billing details;
- Health reports and tests;

- Your healthcare identifier(s) such as your Medicare number, Health Insurance membership number, and/or NDIS participant number;
- Your religious or philosophical beliefs where you choose to divulge these to us and it is directly related to the health services we provide, or seek to provide, to you;
- Your sexual orientation or practices, only when directly related to the health services we provide, or seek to provide, to you.

At or before we collect your health information, we are required to take reasonable steps to ensure that you're aware of your rights to request access to your health information, as well as other information required under the HRIP Act. We will do so through a short statement in our intake form or the email in which we send you this form, and will ensure that this statement provides you with a method of accessing this full Privacy and Confidentiality Manual. We will ensure that this Privacy and Confidentiality Manual is easily accessible to participants and website users.

4.2 Collection and Use of Information

We may collect, hold, use and disclose your personal information for the following purposes:

- To enable you to access and use our Site, associated applications and associated social media platforms;
- To contact and communicate with you;
- For analytics, market research and business development, including to operate and improve our website, associated applications and associated social media platforms;
- To comply with our legal obligations, including NDIS audits, and resolve any disputes we may have.

Where you expressly consent, or consent can be reasonably inferred from your conduct, we may collect, hold, use and disclose your personal information for the following purposes:

- To run competitions and/or offer additional benefits to you;
- For advertising and marketing, including to send you promotional information about our products and services.

If you access, or enquire about, our health services, we may collect, hold and use your personal and health information for the following purposes:

- For internal record keeping and administrative purposes;
- To provide you, or seek to provide you, with our health services;
- At intake, discharge and whenever reasonable, to discuss and determine how to best provide you with our health services by sharing the relevant information between our staff;
- For analytical purposes;
- To meet our legal obligations, including our obligations to participate in NDIS audits;
- To meet our requirements under the HRIP Act which requires us to retain your health information for a period of 7 years since the last occasion on which we provided you with a health service or, if you are under the age of 18 years on that last occasion, until you are 25 years old.

If you're seeking employment with us, we may collect, hold, use and disclose your personal and candidate information in order to assess your eligibility and suitability as a prospective employee.

If we receive unsolicited information from third-parties, we will destroy our copies of the information as soon as practicable and inform the third-party about the breach of privacy.

You may choose not to provide us with some or all of the information that we request from you, however this may affect our ability to provide you with our goods and services, including our health services, which may result in:

- Us not being able to provide you with the goods or services, including health services;
- If the information you choose to provide is in relation to the NDIS or a health insurance provider, we may require you to pay out-of-pocket for health services we provide to you.

All staff contracts include a confidentiality clause. All staff must abide by this Privacy and Confidentiality Manual or face disciplinary, regulatory and/or legal consequences.

4.2.1 Information on Collection of Health Information

Except for in limited legally permitted circumstances, you must be told the following information when we collect your health information:

- How to contact us
- The purposes for which we collect your health information
- Who we usually disclose the information to
- Your rights to access and correct your health information
- The consequences if you don't provide us with your information

We will ensure that this information is available in any intake forms, and we will ensure that the information is provided in person (for example, in our waiting room) as well.

4.3 Disclosure of Information to Third Parties

We may disclose personal (not health or sensitive) information to:

- Third party service providers for the purpose of enabling them to provide their services, including but not limited to – IT service providers, data storage, web-hosting and server providers, debt collectors, maintenance or problem-solving providers, marketing or advertising providers, professional advisors and payment systems operators;
- Our employees, contractors and/or related entities;
- Our existing or potential agents or business partners;
- Sponsors or promoters of any competitions we run;
- Anyone to whom our business or assets (or any part of them) are, or may (in good faith) be transferred;
- Credit reporting agencies, courts, tribunals, regulatory authorities and law enforcement officers:
    - In the event you fail to pay for goods or services we have provided to you; or

  - As required by law, in connection with any actual or prospective legal proceedings, or in order to establish, exercise or defend our legal rights;
- Third parties, including agents or sub-contractors, who assist us in providing information, products, services or direct marketing to you, or to collect and process data such as Google Analytics or other relevant businesses — this may include parties located, or that store data, outside Australia.

4.3.1 Health Information

Use and/or disclosure of your health information is governed by HPPs 10–11. We only use and/or disclose your information where it is legally authorised or required.

We may use and/or disclose your health information between our staff members in order to plan, monitor and adjust our health services, and for internal record keeping and administrative purposes.

We will only use or disclose your health information to third parties on one of the following conditions:

- You consent to the use or disclosure of the health information;
- If you have NDIS funding, in order to provide the NDIA with Assessments and Reports that the NDIA requests;
- If you are funded by Medicare, where we are legally required to provide your referring medical practitioner with information at certain points throughout our course of treatment;
- You would reasonably expect us to use or disclose your health information for a secondary purpose which is directly related to the purpose we collected the information for (for example, to data storage or practice management software in order to provide you with our health services);
- To assist in an emergency where the use or disclosure of your information is reasonably necessary and it is impractical or unreasonable to seek your consent to use the information, or where it is for the purposes of ascertaining the whereabouts of a missing person;
- Failure to use or disclose the health information would place the life, health or safety of you, another person or a child in serious and immediate risk, or would cause a serious threat to public health or safety;
- The use or disclosure of the health information is reasonably necessary for the training of our employees and either the purpose of the use or disclosure cannot be served by the use of de-identified information and it is impracticable for us to seek your consent, or we take reasonable steps to de-identify the information;
- The use or disclosure of the health information is a necessary part of investigating or reporting a matter of potential unlawful activity;
- For law enforcement or investigative purposes, including dispute resolution;
- To anyone to whom our business may be transferred to;
- Where we are legally authorised or required to use or disclose the information, such as:
  - Where the information is subpoenaed by a court;

- We are required to make a mandatory report to the Department of Communities and Justice because we have reasonable grounds to suspect that a child or young person is at risk of significant harm;
- In order to comply with conditions of our NDIS registration, such as by participating in NDIS audits.

4.4 Access To and Correction Of Information

You have the right to request access to your information, and we have a responsibility to ensure that your information is accurate, up-to-date and complete. You can make a request to access or correct your information by email or letter to the contact details provided at the beginning of this document.

4.4.1 Access

You are entitled to request access to your information, and we are required to provide you with access to your information, however limited exceptions apply. When you make a request for access to your information, we are required to respond to your request within a reasonable period of time, which is usually 30 days. If the request is for health information, we must respond to your request within 45 days.

In relation to personal information that is not health information, we will provide you with access to your information without unreasonable expense or delay. However, we will not give you access to the personal information to the extent that the refusal is permitted under APP 12, such as if we reasonably believe that giving access to the information would pose a serious threat to the life, health or safety of any individual, or to public health or safety.

In relation to your health information, we must provide you, or a person you authorise, with access to the information without unreasonable expense or delay. However, we will not give you access to the health information to the extent that the refusal is permitted under the HRIP Act s 29. If we refuse to give you access to your health information on the grounds that providing access would pose a serious threat to your life or health, you may (within 21 days of our refusal) request that we provide the information to a registered medical practitioner nominated by you – we are required to notify you of this right if we refuse you access on those grounds.

4.4.2 Correction

If we are satisfied that the information we hold is inaccurate, out-of-date, incomplete, irrelevant or misleading, or you request that we correct your information, we must take reasonable steps to correct the information. If you make a request to correct your information, we must respond to this request without unreasonable delay.

You may also request that we notify any third-parties which we have disclosed your information to under this Privacy and Confidentiality Manual of any corrections to your information.

In regard to your health information, we must, at your request, make appropriate amendments to ensure that the health information is accurate, up-to-date, complete and not misleading. We may refuse to amend your information on the grounds that we are satisfied that the information is not incomplete, out-of-date, irrelevant, incomplete or misleading, or if we are satisfied that your request contains significant information that is incorrect or misleading. We must notify you of a refusal.

4.4.3 Who Else Can Access Information

We can disclose your health information to a person who is your authorised representative if you are considered incapable of properly consenting to the disclosure of your information because of age, injury, illness or physical or mental impairment, and the disclosure is necessary to provide you with appropriate care or treatment, or otherwise is authorised, permitted or required by law.

4.5 Storage and Destruction of Information

We store some information electronically on Microsoft SharePoint, which is a cloud storage service. We also store information, particularly progress notes, identifying information, some letters, a participant's NDIS plan and other health information, on our practice management software, which is called Splose. All data stored in cloud storage services is kept on servers located within Australia.

Information about vulnerable people (such as mental health information collected through Counselling or Psychology services) is saved in a separate part of SharePoint which only allows access by Management and the Mental Health team. Records of mandatory reports are also saved in a location only accessible to Management. Staff are able to access progress notes and letters relating to non-mental-health clients and their appointments, however Staff who don't deal with client financials are unable to access any invoices or payments for any clients.

Staff are required to have multi-factor authentication enabled on all accounts which can access electronic records.

Where we store your information physically, we take steps to ensure that the information is not accessed by unauthorised persons. Where a staff member is not accessing or using the information, we require all physical information to be locked behind at least two locks on premises (one of those locks being on the external doors).

When we destroy physical copies of information, we do so by shredding the information effectively and disposing of the shredding in a discrete manner.

4.6 Complaints

You can make a complaint regarding our use, disclosure, collection or retention of your information, or any other matters regarding your privacy, in line with our Complaints Policy and Procedure. In summary, you can make a complaint by phone, email, letter or in person by the contact details provided at the beginning of this document.

You can also make a complaint to external bodies/agencies if you are not satisfied with how we have handled your complaint. External bodies you can complain to include:

- The NDIS Quality and Safeguards Commission — Phone 1800 035 544 or TTY 133 677, or visit their website at www.ndiscommission.gov.au
- The Office of the Australian Information Commissioner — Phone 1300 363 992, mail to GPO Box 5288, Sydney NSW 2001, fax to +61 2 6123 5145, or visit their website at www.oaic.gov.au
- The Health Care Complaints Commission — Phone 02 9219 7444, or visit their website at www.hccc.nsw.gov.au

4.7 Employee Information

The personal information of staff members is handled in a different manner to the information of the general public or clients. We have different legal responsibilities, and you have different rights, in relation to your information as an employee.

If you are a current or former employee, you are entitled to request that a copy of any record relating to your employment be made available for you to inspect and copy. We must make a copy of that record available to you as soon as practicable. You may also interview a delegated member of the Management Team at any time during ordinary working hours about a record that we have made or will make.

You have a right to share or not share your pay and your employment terms and conditions. You also have a right to ask other employees about their pay or employment terms and conditions. We will only use and disclose information regarding your pay and employment terms and conditions to the extent necessary to pay you correctly, determine the level at which we should pay you, determine your appropriate employment terms and conditions, and ensure that your employment records are correct.

We have a responsibility to:

- Keep certain records regarding your employment for seven years;
- Ensure that we don't make a record that we know is false or misleading; and to
- Ensure that certain records regarding your employment are kept accurate to the best of our knowledge.

We collect, maintain and keep the following information about you:

- Your personal and emergency contact details, including information to verify your right to work in Australia and to drive a vehicle;
- Information about the terms and conditions of your employment;
- Wage or salary details;
- Leave balances;
- Records of work hours;
- Records of engagement, resignation, disciplining and/or termination of employment;
- Information about training, qualifications, clearances, checks, criminal history, performance and conduct;
- Taxation, banking and superannuation details;
- Union, professional or trade association membership information;
- Health practitioner number or similar registration number and details, such as details of your AHPRA registration;
- Professional indemnity insurance details;
- Email and browsing information and activities whilst on work accounts, premises or in relation to your work;
- Your social media content;
- Vaccination details and confirmation.

4.7.1 Disclosure of Staff Information

We may disclose your employee information to your team leader for their work-related use. This may include informing your team leader of your satisfaction with your role, your clients, and/or your co-workers. We will not do so where we reasonably believe that doing so would cause the work environment to degrade.

Management will always have access to your employee information and records. There may also be members of the internal auditor team who have access to your employee information and records. You can enquire into who has access to your employee records and we will provide you with the names of the person(s) who have access, and the extent to which they have access.

We will only disclose your employee information to external third parties in the following circumstances:

- You consent to the disclosure;
- A Fair Work Inspector has requested the information and we have witnessed their identity card;
- A government agency that has the legal right to access some or all of your employee information (such as the Australian Taxation Office) requests access;
- For law enforcement or investigative purposes, including dispute resolution and for the investigation of potentially unlawful activities;
- A legal permit holder (such as a union official or work health safety inspector) with a right to request access to your information does so;
- The third party directly provides us with a service which requires the use of the employee information, such as a human resources, accounting, or payslip service;
- Failure to use or disclose the employee and/or health information would place the life, health or safety of you, another person or a child in serious and immediate risk, or would cause a serious threat to public health or safety;
- Where we are legally authorised or required to use or disclose the information, such as:
    - Where the information is subpoenaed by a court;
    - We are required to make a mandatory report to the Department of Communities and Justice because we have reasonable grounds to suspect that a child or young person is at risk of significant harm;
    - In order to comply with conditions of our NDIS registration, such as by participating in NDIS audits.

We will also provide employee information to people or organisations who approach us for employment references. We will only provide information which is directly related to your employment with us. We will not provide any sensitive information (for example, medical history) in an employment reference.

If we state that certain information that we collect will be de-identified, for example employee satisfaction surveys, we will take every reasonable step to ensure that the collection and use of the information is in a manner that will not allow you to be able to be identified.

Your nominated emergency contact will be our first point of call if you are for any reason incapacitated or we believe you are at risk of significant harm. We treat the fact that you have nominated an emergency contact as enduring consent to us providing that person with your necessary information if those circumstances occur.

4.8 Monitoring and Review

Management and/or Internal Auditors should review this Manual at least annually and whenever there are major changes to legislation or external guidelines. The process will include a review of any recent changes to legislation, and evaluation of current practices and service delivery types, contemporary policy and practice in the allied health services field, the Incident Register, and will incorporate feedback from relevant stakeholders.

During review the following sources should also be reviewed:

- *Health Records and Information Privacy Act 2002* (NSW)
- *Privacy Act 1988* (Cth)
- *Children and Young Persons (Care and Protection) Act 1998* (NSW)
- NSW Health. *Privacy Manual for Health Information* (2015) 3rd ed. Retrieved from https://www.health.nsw.gov.au/policies/manuals/Pages/privacy-manual-for-health-information.aspx

5 Privacy Data Breach Procedures

A privacy data breach is when any personal information is released in a manner that is inconsistent with this document, or the HRIP Act or APPs, or where there is unauthorised access to or use of any personal information.

Whole Family Health is committed to ensuring any data breaches are swiftly contained and handled in the best manner possible. After any noteworthy data breaches, the Privacy and Confidentiality Manual should be reviewed and any potential improvements to our data breach procedures should be noted in the Continuous Improvement register. Management or the internal auditors may create a go-to guide in relation to common types of data breaches.

Any Staff who become aware of an actual, potential or suspected privacy data breach are to take immediate steps to limit further access to the affected information, such as by recovering physical records from the unauthorised user, or disconnecting a breached computer/system.

Staff must then alert the Managing Director to the data breach or, if the Managing Director is unavailable, any member of Management or an internal auditor.

5.1 Assess & Determine The Potential Impact

Once notified of the potential data breach, the Managing Director must consider whether a privacy data breach has, or is likely to have, occurred and then make a preliminary judgement as to its possible severity. The Managing Director should seek advice from Management and internal auditors where appropriate.

The criteria for determining the severity of the breach are:

- The nature of the affected information, e.g., if it is sensitive information
- The number of individuals affected by the breach
- If the information is protected by any security measures, e.g., password protection or encryption
- Type of person(s) who now have risk
- Whether there is (or could be) a real risk of serious harm to any of the individuals to whom the information relates — if this criterion applies, the data breach is an 'eligible data breach' and the *Privacy Act 1988* (Cth) Part IIIC applies.

5.2 Minor Breach

If a privacy data breach is minor in nature in the opinion of Management, the following steps are to be taken:

- Take any further action to prevent any/any further unauthorised access to or use of the affected information – for example, if the data was accidentally released to an unauthorised third-party, staff should immediately direct the third-party to immediately destroy any copies of the affected data.
- Alert the affected individuals to the data breach. A copy of the alert must be in writing (includes email), and must contain the following information:
    - Whole Family Health contact details

- A description of the data breach
- The kinds of information concerned (it is not necessary to send copies of the information to the affected individual unless they request for this to be done)
- The steps taken to contain the data breach and mitigate the harm that may arise from the breach
- A link to a copy of this manual
- A statement that the individual may make an internal or external complaint which provides them with enough information to allow a reasonable person to do so (for example, the alert may make reference to the copy of this manual and state "You can find information on how to make a complaint in Part 4.6 of that document").

- An Incident Form must be completed within 48 hours of the data breach in line with the Incident Management Policy and Procedure, and must contain:
  - A description of the actual, suspected or potential data breach
  - Summary of action taken in response to the breach
  - Summary of the outcomes of the action taken in response
  - An outline as to why no further action is necessary.

5.3 Moderate to Major Breach

Anything other than a minor breach requires significantly more discretion from the Directors, who must be involved in the management of the data breach as soon as possible. Management and internal auditors must make a recommendation as to whether or not the breach constitutes an 'eligible data breach' and therefore requires a mandatory report to be made to the Office of the Australian Information Commissioner under the *Privacy Act 1988* (Cth) Part IIIC.

6 Revision History

If you have read the entire document previously and it has since been updated, you can read the following notes to see what sections of the document you should review.

6.1 4 May 2023 – v0.1

Author: Geordan Nicholson.

Revision Notes: First draft of the entire document. To be reviewed by Managing Director.

6.2 7 May 2023 – v0.2

Author: Helen Nicholson.

Revision Notes: Reviewed in my capacity as the Managing Director.

6.3 10 May 2023 – v1.0

Author: Geordan Nicholson.

Revision Notes: Final version of the entire document. For publication.