INSTITUTE FOR URBAN INDIGENOUS HEALTH

POLICY

Trust, dignity and autonomy: promoting and respecting the privacy of our Mob (Privacy Policy)

July 2025

institute for urban indigenous health

Version number:	V5.0
Consultation groups:	IUIH Healthcare Quality and Safety Collaborative Committee Privacy and Handling of Personal Information Working Group IUIH Board Performance Quality and Risk Committee
Endorsed by:	IUIH Board
Date endorsed:	18 June 2025
Name and job title of author:	Dr Emma Bell, Manager – Healthcare Quality and Safety
Executive Leadership Team lead:	Dr Carmel Nelson, Clinical Director and Executive Director – Quality and Innovation
Implementation date:	2 July 2025
Last review date:	4 February 2021
Next review date:	2 July 2026
Applicable to:	All IUIH business units, clinics, programs and services

Version control	**Date**	**Author**	**Status**	**Comment**
V5.0	18/06/2025	Dr Emma Bell, Manager – Healthcare Quality and Safety	FINAL	Endorsed by the IUIH Board.
V5.03	30/04/2025	Dr Emma Bell, Manager – Healthcare Quality and Safety	DRAFT	Draft updated to include information about CCTV, mention of tax file number information and inclusion of link to EMPOWA's privacy guideline.
V5.02	18/03/2025	Dr Emma Bell, Manager – Healthcare Quality and Safety	DRAFT	Draft updated to include feedback provided by the Privacy and Handling of Personal Information Working Group and consultation with other teams.
V5.01	15/01/2025	Dr Emma Bell, Manager – Healthcare Quality and Safety	DRAFT	V4.0 required updating to ensure accordance with applicable legislation, The Ways and our organisational values. Initial draft update.
V4.0 (Privacy Guideline)	04/02/2021	Ashleigh Steel, Senior HR Advisor	FINAL	Previous version archived and updated version uploaded. Document manager and owner updated.

V3.0 (Privacy Guideline)	04/02/2021	Ashleigh Steel, Senior HR Advisor	FINAL	Previous version archived and updated version uploaded.
V2.0 (Privacy Guideline)	29/01/2019	Craig Secombe, HR Manager	FINAL	Document category amended.
V1.0 (Privacy Guideline)	04/01/2019	Craig Secombe, HR Manager	FINAL	

Table of Contents

1. Acknowledgement

We honour the many Goori Tribal Nations on whose territories we live and work across South East Queensland (SEQ).

We honour the legacy and the vision of those who paved the way and those who continue to guide us.

We also pay homage to the Torres Strait Islander Nation who have walked this journey with us.

We honour our future generations by maintaining the vision with focused determination.

2. Purpose

IUIH is required by law (*Privacy Act 1988* (Cth)) to have a privacy policy. We recognise that in addition to our legal obligations, we have an obligation to protect the privacy and respectfully handle the personal information of our communities, in accordance with Aboriginal and Torres Strait Islander Frames of Reference, the principles of Indigenous Data Sovereignty, our Cultural Integrity Investment Framework, The Ways Statement, and our values.

This policy supports an open, transparent and culturally responsive approach to promoting and respecting the privacy and handling the personal information of our clients, families, community members, employees, contractors, students, trainees, volunteers and business partners ('our communities') at IUIH. It is for anyone we collect personal information about.

3. The Ways Statement and Cultural Integrity Investment Framework

IUIH's vision of healthy and strong Aboriginal and Torres Strait Islander children, families and communities is supported by our Cultural Integrity Investment Framework and The Ways Statement. The Ways Statement guides our approach to privacy and handling personal information.

- **Ways of Seeing** – our approach to privacy and handling personal information reflects the values and expectations of our communities and supports us to act with integrity and in accordance with our legislative, ethical and cultural obligations.
- **Ways of Knowing** – we strive to ensure our communities have the information they need to make informed choices and exercise autonomy in relation to how we manage their personal information.
- **Ways of Doing** – we strive to ensure that everyone who works at IUIH understands their obligation to protect our communities' privacy and handle their personal information securely, respectfully and lawfully.
- **Ways of Belonging** – we do everything we can to ensure our community members feel safe and comfortable to share their personal information with us and trust that we will handle their personal information in Propa Ways.
- **Ways of Being** – we value, respect and appreciate our community members' capabilities, autonomy and self-determination, including their right to decide if and how they share their personal information with us, to request access to their personal information and raise concerns about how we handle their personal information.

The Ways guide us to take a relational approach to privacy and handling personal information in true partnership with our communities that supports self-determination, personal autonomy, learning, and continuous improvement of our processes. We have a privacy culture that promotes best practice in personal information handling, supports our legal, ethical and cultural obligations, and keeps us accountable to our communities.

4. Legislative and policy context

- *Privacy Act 1988* (Cth) ('Privacy Act')
- *Australian Privacy Principles Guidelines – Privacy Act 1988* (Office of the Australian Information Commissioner)
- *Guide to health privacy* (Office of the Australian Information Commissioner)
- *Indigenous Data Sovereignty Communique* (Maiam nayri Wingara)

5. Indigenous Data Sovereignty

- Indigenous Data Sovereignty is the right of Indigenous people to own, control, access and possess information and data that derive from them.

- IUIH's approach to protecting the privacy and handling the personal information of our communities is grounded in principles of Indigenous Data Sovereignty, recognising that our people have the right to:
    - control how their personal information is collected, stored, protected, used and shared
    - participate in collaborative decision-making that ensures sharing their personal information with us empowers self-determination and autonomy
    - hold us accountable for how we collect, protect, use and disclose their personal information
    - their personal information being used to respect and protect their individual and collective interests.[1]

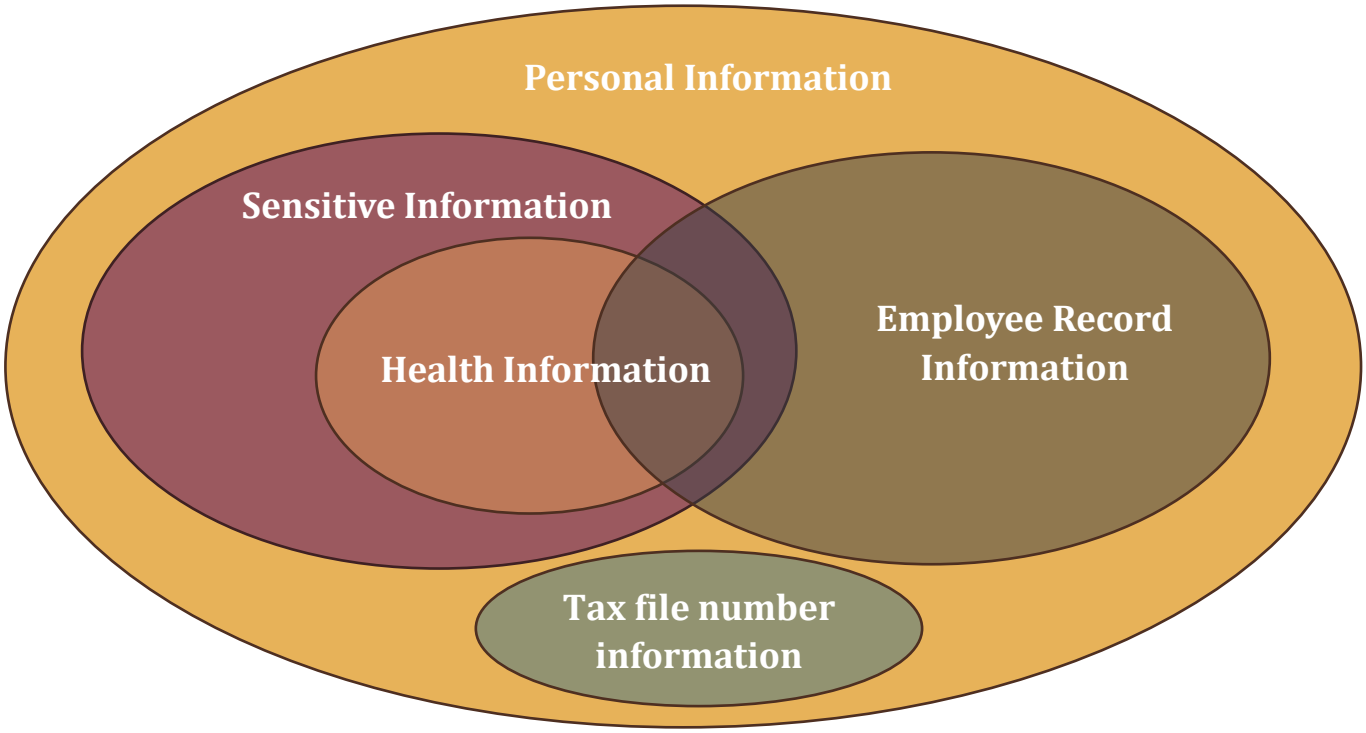
[1] Adapted from: Maiam nayri Wingara. (2018). *Indigenous Data Sovereignty Communique – Indigenous Data Sovereignty Summit, 20 June 2018.* https://www.maiamnayriwingara.org/mnw-principles

6. Principles

7. Kinds of personal information we handle

At IUIH, we handle different types of personal information depending on how you interact with us and the services you access. Figure 1 provides a brief overview of the types of personal information we collect and Table 1 provides more detail about the situations in which we collect and hold personal information and examples of the kinds of personal information we handle.

Figure 1. Types of personal information



- ***Personal information*** is any information or opinion, whether or not it is true, about an identified individual, or an individual who is reasonably identifiable. Personal information can be in any form, including:
    - written or typed, such as letters, emails, text messages, healthcare records, forms, signs, and displays on electronic devices
    - spoken, such as voicemail messages, recordings of conversations, and information shared during a yarn
    - images, such as video recordings, photos, and Closed Circuit Television (CCTV)
    - sign language, gestures, and information shared using alternative and augmentation communication tools such as picture pointing charts, speech generating devices, and eye pointing charts
    - medical information such as DNA obtained from a blood sample.

  An individual may be identifiable from certain information, even if their name, address, date of birth or other similar identifiers are not used. For example, an individual may be identified by a description (for example, 'John's cousin who lives on Jones Street'), a photograph, an audio recording, or a distinctive physical feature (for example, 'That guy with the tattoo of a ship on his forearm').

- ***Sensitive information*** is personal information that includes information or opinion about an individual's:
    - racial or ethnic origin
    - political opinions or associations
    - religious or philosophical beliefs
    - trade union membership or associations
    - sexual orientation or practices

- criminal record
- health or genetic information
- some aspects of biometric information.

- ***Health information*** is personal information that includes information or opinion about an individual's health, illness, injury or disability, including:
  - notes of symptoms and diagnoses
  - information about a health service a person has received or will receive
  - specialist reports and test results
  - prescriptions
  - dental records
  - genetic information
  - wishes about future health services, such as an advance health directive
  - wishes about organ donation
  - appointment and billing details, such as Medicare numbers.

  All information that we collect about people who receive healthcare services through our clinics, programs and services is considered 'health information'.

- ***Employee record information*** is any information kept in an employee record related to current and former employment relationships, including information related to:
  - the appointment of an employee
  - terms and conditions of employment
  - qualifications and licences
  - personal and emergency contact details
  - performance management
  - resignation and termination of employment
  - training, education and development
  - membership of a professional or trade association or trade union membership
  - all kinds of leave
  - tax, banking and superannuation.

  Employee record information for IUIH employees, in certain circumstances, is exempt from the requirements of the Australian Privacy Principles, as outlined in the Privacy Act. However, at IUIH, we choose to apply the Australian Privacy Principles to our employees' records, whilst recognising that there may be times when we need to handle employee record information strictly in accordance with the law.

- ***Tax file number information*** is information that connects an individual's tax file number with that individual's identity.

Table 1. Kinds of personal information we handle at IUIH.

Situations where we collect personal information	**Who do we collect this information from?**	**When do we collect this information?**	**Examples**
Visits to our websites and social media platforms.	Any community member	When someone completes a form or engages with other interactive tools on our websites. When people interact with us on social media.	A person completes a 'feedback' form on our website that includes their name and phone number. Someone provides a comment on one of our social media posts that includes their name and information about their current health.
Events we organise, such as training, conferences, community engagement events, and other community gatherings.	Any community member	When people register for an event or request information about an event. When we take photos or make video recordings of people at our events. When we ask for feedback about an event or community members yarn with us or complete surveys during community engagement events.	Someone's name, phone number, email and dietary requirements provided on an event registration form. A photo of a small group of people at a community event to be used in future marketing materials. A community member gives us feedback about one of our services during a community engagement event and provides their name and phone number so they can be contacted for further information.
General business, such as responding to enquiries and feedback, and corporate functions (for example, finance, contracts, and procurement).	Any community member Contractors Business partners	When someone phones or emails our reception with an enquiry. When we receive and manage feedback about our clinics, programs, services and other operations. When we interact with our business partners (for example, hold meetings, sign contracts).	Someone phones reception to request information about our services and leaves their name and telephone number to be called back. The name, work address and signature of a representative from a funding body who is responsible for signing contracts with us. We arrange for a contractor to attend one of our sites and they provide their name and contact details. Images of people who attend our sites recorded by our CCTV security cameras.

Situations where we collect personal information	Who do we collect this information from?	When do we collect this information?	Examples
Our healthcare and wellbeing services.	Clients Families Community members	When clients register for and attend our clinics, programs and services. When someone is referred to one of our clinics, programs or services by another healthcare provider. When we receive information about a client from another healthcare provider or organisation as part of their care and treatment.	Personal details, such as name, address, date of birth and next of kin. Medicare number. Information in a client's electronic healthcare record, such as symptoms and diagnoses. Prescriptions. A letter from a specialist outlining a treatment plan for a client. Recordings of phone calls to Mob Link. A client's aged care support plan.
Legal service	Clients Families Community members	When someone contacts our legal service or is referred to the service and we provide services to them. When the legal service receives information about a client from one of our clinics, programs or services or another organisation as part of our legal service provision.	Information about a client's health, social and legal history.
Education, traineeship and development programs, such as student placements, POWA (Pathways Our Way Academy) and EMPOWA (our Registered Training Organisation).	Students Trainees Community members Business partners	When we arrange placements at IUIH for students from universities and other education providers. When trainees join our POWA and EMPOWA programs. When we interact with business partners who provide placement and other learning opportunities for our trainees.	A trainee completes a 'Learner Personal Detail Form' that includes their personal information, Indigenous status, and health and disability information. A university provides us with the resume of a potential student. A business partner provides us with feedback about a trainee's performance on placement.

Situations where we collect personal information	Who do we collect this information from?	When do we collect this information?	Examples
Human resources, including job applications and employment related information.	All IUIH employees and prospective employees Volunteers	When someone applies for a job with us, a new employee joins us and an existing employee updates us about their personal information. In the general course of people management, such as carrying out check-ins, performance management, grievance procedures and arranging leave.	A job application received via an online employment service. Notes taken by an interview panel during an interview, including opinions about a candidate's suitability for a role. References provided by referees. Criminal history checks. Outcome of an application for a blue or yellow card. Banking, superannuation and tax file number information. Information about an employee's health, such as current health conditions and medical certificates. Records of check-ins. Records of an employee's leave (for example, annual leave, personal leave, parental leave). An employee's resignation letter.

8. How we collect personal information

- Generally, all personal information we collect is collected directly from the individual, parents/guardians for children and young people, or substitute decision-makers for people who lack decision-making capacity for specific decisions related to collection of personal information (for example, the person's next of kin, emergency contact or enduring power of attorney).

- We may collect your personal information in a number of ways, including:
    - during a yarn – in person or on the phone or video call
    - text message
    - email
    - forms on our websites
    - posts on social media
    - through the websites of our business partners (for example, if you apply for a job through an online employment service that we use, such as Seek)
    - taking photos or making video / audio recordings (for example, images collected by CCTV).

- When we collect sensitive and health information, we will generally ask for your consent first.

- There are some situations where we may collect sensitive and health information without your consent, such as in an emergency situation where we urgently need information about you to keep you well or safe and there isn't time to ask for consent (for example, if you become seriously unwell during your first visit to one of our clinics and we urgently ask your usual doctor about your medical history and current medication).

- We may collect personal information about you from other people or organisations in some circumstances. Examples of this include:
    - you are referred to one of our clinics, programs or services and your personal information is provided by the referrer
    - requesting information about your health history from a responsible person, such as a relative or friend, if they attend an appointment with you or if you are unable to provide the information yourself
    - your My Health Record, Queensland Health Viewer record, Australian Immunisation Register record, National Cancer Screening Register records and MyMedicare registration
    - you are planning to attend one of our health promotion, community engagement or other events and your personal information is provided by an organisation arranging your involvement, such as a school, community organisation, or your employer
    - you apply for a job with us and we request a reference from one of your referees.

9. Why we handle personal information

We handle personal information for many different purposes, including:

- to provide services to support our communities' health and social and emotional wellbeing, including liaising with other healthcare and support organisations to ensure care is comprehensive, holistic and coordinated
- to provide legal services to clients
- to evaluate, monitor and improve our healthcare services
- managing Medicare payments
- professional supervision and mentoring for our staff
- to administer human resources and payroll functions for our employees
- plan, run and evaluate health promotion activities, community engagement events, conferences and other community events
- developing website content and social media posts
- developing education, training and development materials
- marketing our clinics, programs and services
- developing health promotion materials
- responding to feedback and complaints

- contributing to consultations about our services such as comments on our websites or social media platforms
- processing requests to access and/or correct personal information we hold
- reviewing healthcare and workplace health and safety incidents
- monitoring visitors to and activity on our websites and social media platforms
- research.

10. How we store and protect your personal information

General

- We keep a register of personal information we hold at IUIH and review and update it regularly, so:
    - we know the kinds of information our teams collect and hold, how they store and protect it and who has access to it
    - we can regularly consider the risk of your personal information being misused, interfered with, lost, changed, disclosed or accessed by people who should not have access and take action to reduce any risk.

- If you ask us not to share your personal information with particular individuals or organisations, we will respect your decision (unless a lawful exception applies).

- When our employees sign employment agreements, they confirm they will keep confidential information (this includes personal information) secret while they work with us and when they are no longer employed by us.

- We only allow certain staff to access certain personal information. Access to our systems for storing personal information is provided on a strictly 'need to know' basis. In general, staff who are authorised to access these systems sign agreements stating they will only access these systems for very specific purposes. For example, our healthcare workers sign agreements stating they will only access the electronic healthcare records of clients for the purpose of providing care and will not access client records unless there is a healthcare-related or administrative reason to do so.

- We hold personal information in both paper-based and electronic forms. We make every effort to store personal information electronically where possible and destroy paper records where appropriate. Where we hold personal information in paper-based records, we store these securely in lockable filing cabinets / drawers and lockable offices.

- All personal information we hold is stored in data centres in Australia. If we share information with other organisations or agencies, we cannot guarantee that they will store that information in Australian-based data centres.

Health information

- The health information of our clients is held securely in our electronic health information systems.

Employee record information

- Employee record information is held securely in our electronic human resource management systems, our electronic payroll and finance systems and other secure electronic locations accessible by managers of our business units, clinics, programs and services.

- IUIH uses a range of online employment services to advertise jobs and manage job applications. If you apply for a job with us via one of these services, you will share your personal information with that service via their website. All services should have a privacy policy available on their website that will provide information about how they handle your personal information.

Legal services

- Our legal service uses secure electronic records systems to store the personal information of clients of the legal service and the family mediation service. Legal service and family mediation service records are held in separate electronic systems.

- All personal information of clients collected and held by our legal service and family mediation service is stored separately from other client information. For example, legal service and family mediation service employees do not have access to our health information systems and employees outside the legal service do not have access to the legal service and family mediation service electronic records systems.

Tax file number information

- Tax file number information is held only in our secure electronic HR and payroll systems and is accessible only by HR and payroll staff.

Trainees

- Personal information of our trainees is held securely in electronic systems by our POWA and EMPOWA teams and is only accessible by employees who work in these teams.
- EMPOWA's privacy policy is available here.

11. Anonymity

- You have the option of interacting with IUIH anonymously (without telling us your name or any other identifying information) or using a pseudonym (a name that is different to your real name), if this is reasonably possible in the circumstances. For example, you may wish to make an anonymous complaint about one of our services, phone our reception with a general enquiry about the location of our clinics without giving your name, give us feedback at a community engagement event without telling us your name, or engage with our websites or social media platforms with a user name that is not your real name.

- In most situations, we are likely to need to know your name, contact details and enough information to allow us to deal with your issues effectively. For example, if you attend one of our clinics, we need to know your name and Medicare number if you want to be bulk billed.

- If you tell us you would like to deal with us anonymously or using a pseudonym, we will always consider this and yarn with you about the potential risks and benefits, although there will be situations where we may not be able to agree to your request.

12. How we use and disclose your personal information

- We only use and disclose your personal information for the specific purpose/s for which it was collected. If we wish to use your personal information for a different purpose, we will ask your permission first (unless a lawful exception applies).

- If personal information we hold is used for research, procedures for handling this information must meet strict ethical requirements and be authorised by one of our senior leaders. We will always try to ask for your consent to use personal information for research purposes if possible, but sometimes when it is not possible to ask for consent, we may be allowed to use personal information for research without consent. For example, if we are participating in a research project that requires access to the healthcare records of people with diabetes, we may no longer have the correct contact details for all relevant clients. When we are considering using personal information for research purposes without consent, we undertake a careful risk assessment, including considering what our communities' expectations would be and take into account the views expressed during community engagement yarns.

- Sometimes it may be necessary to disclose your personal information without consent, such as:
    - to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or public safety (for example, a paramedic is transporting one of our clients with a serious health concern to hospital and requires information from us about the client's medical history)
    - taking appropriate action in relation to suspected unlawful activity or serious misconduct (for example, an internal investigation of potential fraud by an employee)
    - locating a missing person (for example, the police request information from us that may assist in locating one of our clients who has been reported missing)
    - managing a legal claim or participating in confidential mediation or other alternative dispute resolution (for example, if we participate in mediation and disclose personal information about individuals as part of that process)
    - other situations allowed by law (for example, in response to a court order).

- We may disclose information about our clients to other healthcare providers or support agencies but we will generally ask for consent first.

Deidentified information

- When information that identifies a person has been permanently removed from a particular piece of information, or never included, this information is 'deidentified'. Examples of deidentified information include:
    - a database that includes information about access to one of our services, but only includes a randomly generated client identification number, the suburb where the client attended the service, and how many times the client accessed the service
    - a photograph that has been blurred so a person is not able to be identified
    - an extract from a healthcare record where the client's name and other personal details have been removed
    - research findings that are presented about groups of clients (for example, clients diagnosed with type 2 diabetes) without any identifying information about individuals.

- IUIH uses deidentified information for the following purposes:
    - reporting to organisations and agencies that fund our programs and services
    - sharing information we have gathered through community engagement yarns to improve our services
    - research
    - evaluating our services
    - teaching and learning.

- We acknowledge that our communities expect to maintain control over their data and its use and expect us to protect, manage and share their data in accordance with their values and principles of Indigenous Data Sovereignty. Even when information or data does not identify individuals, we take steps to ensure:
    - we ask for consent to use and share information and data wherever possible and practical
    - data and information is only used for the benefit of Aboriginal and Torres Strait Islander people
    - data and information is not exploited, misinterpreted or used to perpetuate negative stereotypes
    - we engage with and educate our communities regarding how their information and data can be used for their benefit and alleviate concerns about misuse
    - there are robust, Indigenous-led data governance mechanisms in place at IUIH that respect cultural authority and ensure data is managed in line with community values and protocols
    - Elders are recognised as crucial data custodians.

Information about specific clinics, programs and services

- When you interact with one of our clinics, programs and services, they will give you more specific information about how they collect, store, protect, use and disclose your personal information. If you have

questions about how our clinics, programs and services handle your personal information, you can ask someone from the particular clinic, program or service you are in contact with, or you can contact:
IUIH's Privacy Leader
Email: *privacy@iuih.org.au*
Telephone: *07 3828 3600*
Post: *IUIH, 22 Cox Road, Windsor, QLD, 4030.*

13. Quality of personal information

- We are committed to ensuring all personal information we hold is accurate, up-to-date and complete. We act to update or amend your personal information promptly when we become aware that changes are needed.

14. Destruction and deletion of personal information

- We securely destroy and delete personal information when it is no longer needed or when we are required to or allowed to by law.

- Sometimes we may remove information that identifies individuals and keep information in this deidentified form. Once information no longer identifies an individual, it is no longer considered to be 'personal information'.

15. Our websites and social media platforms

Websites

- Our websites – www.iuih.org, www.moretonatsichs.org.au, deadlychoices.com.au and empowatraining.org.au – are hosted in Australia.

- When you visit our websites, we collect data using Google Analytics, Google Ads and Microsoft Clarity. These applications help us to learn about how people use our websites by giving us information such as the number of people who access our websites, how long they spend on the website, the pages they visit, general information about their location and information about their browsers and devices. These applications generally do not capture information that would identify you.

- We use Google reCAPTCHA on some of our websites to protect against misuse of our websites. Google reCAPTCHA collects data about you when you interact with forms on our websites, including mouse movements, information about your browser and devices, and general information about your location. Google reCAPTCHA does not collect any information that you enter into forms on our websites and generally does not capture information that would identify you.

- The forms on our MATSICHS and EMPOWA websites do not store any personal information. Information submitted in these forms is sent via email directly to our Communications Team.

- We use JotForm to manage forms on our Deadly Choices website. JotForm collects information that you provide via forms on the website and may transfer it outside Australia. JotForm's privacy policy is available here.

- Our 'YarnItUp' platform, an online tool we use to engage with our communities, is owned and operated by us using software licensed from an organisation called Social Pinpoint. Personal information collected via YarnItUp is used by IUIH to provide information about services, collect feedback about our services and to consult with our communities about new initiatives and service developments. We handle personal information collected via our YarnItUp platform in accordance with this policy. Social Pinpoint may also access personal information collected via YarnItUp in accordance with their privacy policy, which can be accessed here.

Cookies

- Cookies are small data files that are created when you visit our websites and are stored on your devices. Cookies are used for record-keeping purposes and to improve your experience of using our websites.

- Information collected using cookies usually will not be personal information, because we will not be able to identify you from this information.

- Most internet browsers give you the option to accept or not accept cookies. If you do not want to accept cookies, you can set your browser preferences to reject all cookies.

Mailing lists and direct marketing

- We ask for your consent before you are included on any of our mailing lists or receive any other form of direct marketing, such as phone calls. We might ask for your consent during a yarn, through ticking a box when you register for one of our services or an event, or by signing a form.

- You can choose not to be on our mailing lists or receive direct marketing. Even if you have previously told us you want to be on a mailing list or receive direct marketing, you can always change your mind later. If you no longer want to be on a mailing list or receive direct marketing, you can:
    - reply using the contact details in the message and say you no longer want to be on the mailing list
    - tell us during a phone call that you don't want to be called anymore
    - use the 'unsubscribe' link in an email if there is one
    - directly contact the clinic, service or program that sent you a message or called you
    - contact *IUIH's Privacy Leader at: email privacy@iuih.org.au; telephone: 07 3828 3600; post: IUIH, 22 Cox Road, Windsor, QLD, 4030.*

- We use an application called Vision6 to manage mailing lists. Vision6 helps us send out information via email and text message and collects information such as whether you opened an email from one of our mailing lists, which links you click in an email, the application you use for email (for example, Outlook or Gmail), information about your device and general information about your location. Vision6's privacy policy is available here.

Event registration

- When you register to attend one of our events, we collect personal information such as your name, email, telephone number and dietary requirements.

- We use an application called StickyTickets to manage our event registrations. StickyTickets collects the personal information that you provide when you register for an event. You can view StickyTickets' privacy policy here.

Surveys

- Some of our teams use online surveys to gather feedback about our services and for research and community engagement, which may include personal information that you provide when you respond to a survey.

- We use Qualtrics to manage our online surveys. Qualtrics' privacy policy is available here.

Social media platforms

- IUIH uses X (formerly known as 'Twitter'), Facebook, YouTube, Instagram and LinkedIn to provide information about our services, general health and wellbeing advice and important health alerts.

- When you interact with our social media platforms, we collect any personal information you provide.

- Personal information posted on social media is covered by each platform's privacy policy, which are available via these links: X; Facebook; You Tube, Instagram; and LinkedIn.

Artificial intelligence (AI)

- IUIH acknowledges that AI is a growing and rapidly evolving part of our work. Our use of AI is changing quickly, and we are constantly updating our guidelines and advice to employees about use of AI.

- We currently do not permit any personal information to be shared with or through AI tools or applications.

- If you would like more information about how we use AI at IUIH and how we keep your personal information safe, please get in touch at privacy@iuih.org.au.

16. CCTV

- Some of our sites are equipped with CCTV cameras. We use CCTV to monitor our sites and promote the safety and wellbeing of our communities.

- Our CCTV cameras only record video images (not audio / sound) and these are stored in a secure electronic system that is only accessible by our infrastructure and logistics, workplace health and safety, security and IT teams.

- Images recorded via CCTV are only viewed if there is a need to do so, such as if an incident is reported at one of our sites. Only staff directly involved in responding to incidents or other issues will view CCTV images.

- The images from our CCTV cameras are generally stored for 30 days and then deleted.

- If you have questions about how we use CCTV, you can contact:
  IUIH's Privacy Leader
  Email: *privacy@iuih.org.au*
  Telephone: *07 3828 3600*
  Post: *IUIH, 22 Cox Road, Windsor, QLD, 4030*

17. How personal information can be accessed and corrected

- Everyone whose personal information we hold has the right to request access to their personal information and correction of their personal information.

- You can ask to access or correct your personal information any way you want, as long as we can clearly and safely identify you. Requests made in writing are best if possible but we can talk on the phone, video call or have a yarn in person. We will need to verify your identity and if you are acting on behalf of someone else, verify you have permission to do so. We aim to respond to requests, provide the information or make corrections within 30 days of receiving the request.

- You can ask to access or correct your personal information by contacting:
  IUIH's Privacy Leader
  Email: *privacy@iuih.org.au*
  Telephone: *07 3828 3600*
  Post: *IUIH, 22 Cox Road, Windsor, QLD, 4030*

- When you make a request to access or correct your personal information, we need the following information:
  - your name and contact details

- the personal information you want to access or correct (this should be as specific as possible, for example, 'the record of my GP appointment on 30 June', or 'You have my name wrong in the email you sent me on 12 July')
- how you would like to access your personal information (for example, look at it on a computer at one of our sites, post, email)
- if there is someone acting on your behalf, their name and contact details.

- If we decide not to grant your request to access or correct your personal information, we will let you know the reasons for this in writing and tell you how you can complain or ask for more information about our decision. Sometimes we might not grant a request to access or correct personal information if:
  - giving you access would pose a serious threat to the life, health or safety of any individual or to public health or public safety
  - giving you access would have an unreasonable impact on the privacy of others
  - we think the request might not be serious or is intended to harass or intimidate our employees (for example, the request contains offensive or abusive language)
  - you have made many similar requests and the relevant information has already been provided to you
  - your personal information is part of, or expected to become part of, legal proceedings between you and us
  - giving you access would be unlawful
  - giving you access would be likely to interfere with investigating unlawful activity or misconduct
  - giving you access would reveal commercially sensitive information.

- We never charge a fee to people just to ask for access to their personal information. We may charge for giving access to the requested personal information if giving access involves significant staff or administrative costs, such as time taken to locate and retrieve the information, copying and printing materials, and postage costs. We will always tell you in advance if there is likely to be a cost for providing access to the personal information you request and what the cost is likely to be.

18. How you can complain and how your complaint will be handled

- If you are worried about how we have handled your personal information and want to make a complaint, you (or someone who has permission to act on your behalf) can let us know by contacting:
  IUIH's Privacy Leader
  Email: *privacy@iuih.org.au*
  Telephone: *07 3828 3600*
  Post: *IUIH, 22 Cox Road, Windsor, QLD, 4030*

- We accept complaints about how we handle personal information in any way including by telephone, video call, email, letter or in person. If you raise a concern about how we have handled your personal information with someone other than our Privacy Leader, the person you yarn with will pass on your complaint to the Privacy Leader.

- Your complaint will be investigated by IUIH's Privacy Leader and senior managers in accordance with our complaints policy (you can ask us for a copy of this policy).

- We aim to respond to your complaint within 30 days.

Complaining to the Office of the Information Commissioner

- If you have complained to us about how we have handled your personal information and we don't respond within 30 days or you are unhappy with our response, you can complain to the Office of the Australian Information Commissioner. You must complain to the Office of the Australian Information Commissioner in writing – they are unable to accept complaints any other way.

- The Office of the Australian Information Commissioner can accept written complaints:
  - through their online privacy complaint form
  - on a privacy complaint form that you download from their website and complete
  - in a letter (GPO Box 5288, Sydney, NSW, 2001) or fax (02 61235145).

19. Overseas disclosure

- In general, we don't disclose your personal information overseas.

- There may be very limited situations where this is necessary, such as:
  - a client moves overseas and requests access to their healthcare records
  - we receive a complaint from someone who is located overseas
  - a client's next of kin needs to be contacted and is located overseas
  - a client is taken to hospital while overseas on holiday and we are asked by an overseas healthcare provider for information about the client's medical history.

- When you interact with us through our social media platforms and websites hosted by our business partners, those platforms and websites (and other organisations associated with them) may collect and hold your personal information overseas.

20. Updates to this policy

- We review this policy annually and any updated versions will be made available:
  - on our websites
  - in our internal quality management system.

- This policy was last updated on 2 July 2025.

- You can ask us for a copy of this policy in a different format (for example, a paper copy) or ask any questions about this policy by contacting:
  IUIH's Privacy Leader
  Email: *privacy@iuih.org.au*
  Telephone: *07 3828 3600*
  Post: *IUIH, 22 Cox Road, Windsor, QLD, 4030*