Policy – Privacy and Confidentiality

Version No.	Approval Date	Next Review Date	Document Owner	Authorising Group
9.0	July 2025	July 2030	GM People Governance and Community (GQ&R)	ELT

Review History

Version No.	Version Date	Summary of Changes	Author
1.0	August 2003	Policy Created	CEO
2.0- 4.0	August 2014	Various Updates	CEO
4.1	December 2017	Transferred to new template Procedure sections transferred to Procedure template	EA to CEO
5.0	March 2019	Included relevant Legislations	Q&R
6.0	September 2021	Procedure- Notifiable Data Breaches added to Associated frameworks, policies, procedures and guidelines	Q & R
7.0	June 2022	Include definitions in disclosure statement that reflects consent form following recommendations from external review for Forensic client project	GQR
8.0	November 2024	To include guidance on AI in clinical applications	GMFCS
9.0	April 2025	Formally Privacy and Confidentiality of Client Information: To change name and make wider than just client information, remove detailed section on AI to put in its own Policy Major review by legal counsel	GMFCS Health Legal – external legal consultant GQR

Table of Contents

1. Target Audience

IPC Health Staff, Board of Directors, Contractors, Students, Volunteers and Clients.

2. Definitions

Australian Privacy Principles (APP)	The APPs are the thirteen principles contained in schedule 1 of the *Privacy Act 1988* (Cth) that set out the minimum standards regulating how large businesses, health service providers and some small businesses and non-government organisations may handle individuals' personal information. The APPs cover the collection, use, disclosure and storage of personal information. They also allow individuals to access that information and have it corrected if it is wrong.
Health Privacy Principles (HPP)	The HPP's are the eleven principles contained in the *Health Records Act 2001* (Vic) That set out the minimum standards regulating the collection, use, disclosure and storage of 'health information' that is held by public and private sector organisations.
Health Information (*Health Records Act 2001* (Vic))	Means information or an opinion, whether true or not, about the physical, mental or psychological health of an individual, their disability, and includes 'personal information' collected while receiving health services.
Confidential Information	Means any Information at any time disclosed directly or indirectly to IPC Health or its Personnel by the Disclosing Party or its employees, agents, consultants and advisers, and any extracts, summaries or analyses thereof prepared by or on behalf of the Recipient except to the extent that such Information: • is or becomes generally available to the public other than as a result of a disclosure by the Recipient or any employee, agent, consultant or adviser to the Recipient; • was available to the Recipient on a non-confidential basis prior to its disclosure by the Disclosing Party or its employees, agents, consultants or adviser; or • becomes available to the Recipient on a non-confidential basis from a person who, to the actual knowledge of the Recipient, is not otherwise bound by a confidentiality agreement with respect to such information, or is not otherwise prohibited from transmitting the information to the Recipient.
Personal Information	Information or an opinion about an individual whether it is true or not where that individual's identity can be ascertained from the information or opinion and includes name, address, telephone number, .
Consent	Means the agreement of a client or their authorised representative to a proposed action e.g. collection and use, disclosure, transfer of information or for particular treatment. Consent may be explicit or implied however, it must be informed, specific, voluntary and given by a client or their representative with a legal capacity to do so.
Legal Capacity	Refers to a person's ability to make decisions regarding the specific matter for which informed consent is being given. All adults are presumed to have capacity, and capacity may change over time and capacity must be considered each time a decision is made.
Data Security	Relates to measures that are put in place to protect the integrity, availability and confidentiality of information, whether paper based or computerised. Security measures are in place to protect against accidental damage, misuse and unauthorised access or disclosure.
Privacy Officer	Means the IPC Health Chief Executive Officer or their delegate
Sensitive Information	Means: (a) information or an opinion about an individual's: (i) racial or ethnic origin; (ii) political opinions; (iii) membership of a political association; or(iv) religious beliefs or affiliations; (v) philosophical beliefs; (vi) membership of a professional or trade association; (vii) membership of a trade union;

	(viii) sexual preferences or practices; (ix) criminal record; that is also personal information; (b) health information about an individual; (c) genetic information about an individual that is not otherwise health information.
Personnel	In this policy defined as Staff, Board of Directors, Contractors, Students and Volunteers
Australian Privacy Principles (APP)	Are contained in schedule 1 of the *Privacy Act 1988* (Cth) that set out the minimum standards regulating how large businesses, health service providers and some small businesses and non-government organisations handle individuals' personal information. The APPs cover the collection, use, disclosure and storage of personal information. They also allow individuals to access that information and have it corrected if it is wrong.
Confidential Information	Means any Information at any time disclosed directly or indirectly to IPC Health or its Personnel by the Disclosing Party or its employees, agents, consultants and advisers, and any extracts, summaries or analyses thereof prepared by or on behalf of the Recipient except to the extent that such Information: • is or becomes generally available to the public other than as a result of a disclosure by the Recipient or any employee, agent, consultant or adviser to the Recipient; • was available to the Recipient on a non-confidential basis prior to its disclosure by the Disclosing Party or its employees, agents, consultants or adviser; or • becomes available to the Recipient on a non-confidential basis from a person who, to the actual knowledge of the Recipient, is not otherwise bound by a confidentiality agreement with respect to such information or is not otherwise prohibited from transmitting the information to the Recipient.
Consent	Means the agreement of a client or their authorised representative to a proposed action e.g. collection and use, disclosure, transfer of information or for particular treatment. Consent may be explicit or implied however, it must be informed, specific, voluntary and given by a client or their representative with a legal capacity to do so.
Data Security	Relates to measures that are put in place to protect the integrity, availability and confidentiality of information, whether paper based or computerised. Security measures are in place to protect against accidental damage, misuse and unauthorised access or disclosure.
Health Information (*Health Records Act 2001* (Vic))	Means information or an opinion, whether true or not, about the physical, mental or psychological health of an individual, their disability, and includes 'personal information' collected while receiving health services.
Health Privacy Principles (HPP)	Are contained in Schedule 1 of the *Health Records Act 2001* (Vic) that set out the minimum standards regulating the collection, use, disclosure and storage of 'health information' that is held by public and private sector organisations.
Legal Capacity	Refers to a person's ability to make decisions regarding the specific matter for which informed consent is being given. All adults are presumed to have capacity, and capacity may change over time and capacity must be considered each time a decision is made.
Personal Information	Means information or an opinion about an individual whether it is true or not where that individual's identity can be ascertained from the information or opinion and includes name, address, telephone number .
Personnel	For the purposes of this policy, Personnel means IPC Health Staff, Board of Directors, Contractors, Students and Volunteers.
Privacy Officer	Means the IPC Health Chief Executive Officer or their delegate.
Sensitive Information	Means: (a) information or an opinion about an individual's: i. racial or ethnic origin; ii. political opinions; iii. membership of a political association; or(iv) religious beliefs or affiliations;

	iv. philosophical beliefs; v. membership of a professional or trade association; vi. membership of a trade union; vii. sexual preferences or practices; viii. criminal record; ix. that is also personal information; (b) health information about an individual; (c) genetic information about an individual that is not otherwise health information.

3. Policy statement

A person's right to the protection of their privacy from unlawful or arbitrary interference is a fundamental human right, protected by Commonwealth and State government laws. The consequences of breaching consumer privacy are serious and can include sanctions and penalties under both criminal and civil laws as well as disciplinary action.

IPC Health is committed to protecting the privacy of all personal, sensitive and/or confidential information collected, used, stored, and disclosed as a necessary part of delivering high-quality healthcare services. This extends to both electronic and hard-copy records, including records of correspondence such as e-mail, phone and verbal conversations that are captured.
IPC Health complies with the following legislation and privacy principles:

- Privacy Act 1988 (Cth) and the Australian Privacy Principles
- Health Records Act 2001 (VIC) and the Health Privacy Principles
- Privacy and Data Protection Act 2014 (Vic) and the Information Privacy Principles
- (Relevant Privacy Laws)

All Personnel have a responsibility to ensure that the privacy of all personal, sensitive and/or confidential information is protected, confidentiality is maintained, and client and employee information is only accessed for the purpose of performing their duties as an IPC Health employee.
All Personnel are required to sign a confidentiality agreement (as part of on-boarding), participate in privacy and confidentiality training as directed, and adhere to the IPC Health Codes of Conduct.

4. Policy principles

4.1 Confidentiality

- Personnel must treat Confidential Information as secret and confidential, and to protect its secret and confidential nature, to refrain from disclosing, publishing or communicating any of the Confidential Information which the Personnel receives to any third parties except:
    - to such of its employees, agents, consultants or advisors who have a need to know such information in connection with the performance of their duties and have been advised of the confidential nature of the Confidential Information and IPC Health's obligations under this Policy;
    - to any governmental, regulatory or administrative agency, authority board or body having jurisdiction over IPC Health, where such disclosure is required in accordance with applicable law; and
    - where disclosure to any other person is required by law pursuant to subpoena or other process, whether legal, administrative or other.
- Personnel will sign the relevant Deed of Confidentiality.
- Intended disclosure or suspected breaches of confidentiality should in the first instance be discussed with the relevant Manager.

4.2 Privacy - Collection

IPC Health Personnel must:

- only collect Personal Information and/or Health Information where it is reasonably necessary for IPC Health's functions in providing health services to a person (**the primary purpose**)
    - collection will be fair, lawful and non-intrusive
    - collection is with the person's consent or that collection is in accordance with the law;
    - wherever possible Personal Information and/or Health Information will only be collected directly from the client rather than from third parties.
    - where Personal Information and/or Health Information is collected from a third party, it should be with the client's consent, unless:
        - the person is a child;
        - in an emergency or where the health, safety or welfare of the person or another person or the public is at risk;
        - where the person is unable to consent due to a medical condition or they lack Capacity
        - it is from an authorised legal representative or carer or an external service provider.
- take reasonable steps to ensure that the person is made aware of the details of collection, including the purpose for which their Personal Information and/or Health Information is being collected and how it will be used.
- not collect Sensitive Information unless:
    - The individual has consented, and the Sensitive Information is reasonable necessary or directly related to IPC Health's functions.

4.3 Privacy - Use and Disclosure

- IPC Health will take reasonable steps to ensure Personal Information and/or Health Information is kept confidential.
- IPC Health Personnel must only use Personal Information and/or Health Information for the primary purpose for which it was collected, or a secondary purpose that is directly related to the primary purpose and the person would reasonably expect their Personal Information and/or Health Information to be used for that related secondary purpose, e.g. where a person is being transferred to the care of a different service provider and Health Information is shared with that provider.
- IPC Health Personnel must not disclose Personal Information and/or Health Information unless:
    - the client consents to the disclosure;
    - disclosure is:
        - required or permitted by law, for example: under a validly issued subpoena, mandatory reporting obligations, in an emergency where there is a serious risk to the health, safety or welfare of an individual or the public.
        - necessary in order to ensure clients are receiving the most appropriate treatment, such as for the provision of necessary emergency treatment
- IPC Health Personnel will keep the client informed to whom, how and why their information is disclosed and the consequences for the client if the information is not provided to the third party.

4.4 Information Sharing Schemes

Personal Information and/or Health Information may be disclosed in some cases without consent in accordance with Family Violence Information Sharing Scheme (**FVISS**) or Child Information Sharing Scheme (**CISS**).

NB these are permitted disclosures in accordance with law

Refer to **IPC Health's Information Sharing Procedures** for further information.

4.5 Data Quality, Security & Retention

- IPC Health will take reasonable steps to ensure that the Personal Information and/or Health Information that is holds is accurate, complete and up to date.
- IPC Health must:
    - ensure data contained within information or patient management systems is stored securely with permission access levels monitored and managed
    - take reasonable steps to protect personal information from misuse, interference, loss, unauthorised access, modification or disclosure. Information will be kept secure and confidential
    - require contractors and third-party providers to sign confidentiality agreements or enter contracts with confidentiality terms which bind them to protect the confidentiality of sensitive information to no lesser extent than if they were an employee
- IPC Health Personnel must:
    - Ensure that they do not allow sensitive information to be visible on screens or left in places (including locations outside IPC Health) where it may be viewed or accessed by members of the public or employees whose duties do not require them to access this information
    - Ensure that Sensitive Information is only transmitted externally via authorised PKI data encryption systems. If in doubt, Personnel must check with their manager prior to sending information
        - Sensitive Information must not be transmitted externally via e-mail.
- IPC Health will ensure it has processes:
    - to archive, de-identify and/or destroy Personal Information and/or Health Information in accordance with relevant disposal and retention schedule laws when the information is no longer required, including Public Records Office Victoria Disposal and Retention Schedules;
    - to report any breaches in the incident management system;
    - to conduct audits:
        - periodically of records and databases to ensure that the information held is accurate and up to date; and
        - to prevent and detect unauthorised access and fraud;
    - to securely store physical or paper records and ensure they can be accessed only by authorised personnel;
    - to ensure computer systems uniquely identify individual users to ensure that access is appropriately authorised.

4.6 Openness and Transparency

- IPC Health will:
    - make this policy available on IPC Health's website, internal controlled document system, and hard copy if requested.
    - provide people with information to support their consent to information collection; even in instances where information must be collected for service provision to occur.
    - take all necessary steps to ensure that the consumer health information that is collected is accurate and up to date and relevant to IPC Health's activities
    - ensure that any suspected infringements of privacy are thoroughly investigated and are reported as an incident.

4.7 Access and Correction

- Any request by the individual or any other person to access and sight a file must be authorised by the IPC Health Privacy Officer.
- Access to client files and requests for copies of client files, must only be given in accordance with the Relevant Privacy Laws.

- where possible, access should be provided as requested by the client – this may be to view documents, receive documents or to have information explained verbally.

- Where a client has accessed their file the type of access is to be documented in the client's file.
- IPC Health is not obliged to re-format or summarise material in response to an access request. However, if the Privacy Officer believes a summary may be more helpful, a summary may be offered instead, this is by mutual consent.
- IPC Health may refuse access to a client's Health Information where:
  - Providing access would pose a serious threat to the life or health of any person;
  - Providing access would have an unreasonable impact on the privacy of other individuals;
  - the information is subject to legal proceedings or likely to prejudice law enforcement functions; is exempt; denying access is required or authorised by law; or the information has already been provided.
- If the client is able to establish that Health Information held by IPC Health is inaccurate, incomplete, misleading or out of date, IPC Health must take reasonable steps to correct the information. deems that the information held is inaccurate, incomplete or misleading they have the right to request correction to the health record.

NB IPC Health must not delete information unless deletion is permitted, authorised or required by law; or it is not contrary to law and the deletion occurs more than seven (7) years after the last occasion on which health services were provided or the health Information was collected when the individual was a child and the individual has attained the age of 25 years, whichever is the later.

4.8 Identifiers

- A unique registration number will be allocated to each client's details to enable the organisation to conduct its functions efficiently.
- identifiers assigned by the Commonwealth Government including Medicare or DVA numbers, cannot be used by IPC Health as identifiers for their clients.
- IPC Health will only collect, use or disclose these identifiers where it is necessary to meet the functions of the organisation such as determining eligibility, creating a health record, charging fees or reporting to funding bodies.

4.9 Anonymity and Pseudonymity

- Where it is practicable and lawful, individuals have the option of not identifying themselves to IPC Health by using an alias when seeking health care.
- In some situations it may not be lawful or practicable to provide a service to those who choose to remain anonymous.
- Factors that affect the decision on anonymity or use of an alias include:
  - Whether identification is required under legislation for example, diagnosis and reporting of a notifiable disease.
  - Whether the quality or timeliness of health care could be jeopardised
  - Billing for medical or dental services.
  - Request for general enquiry

4.10 Trans-border Data Flow

- IPC Health Personnel must ensure that all Personal and Health Information is stored wholly within Australia.
- Where it is necessary to transfer health or other sensitive information to a place outside Victoria, IPC Health will only do so with consent, or where the transfer is authorised or required by law.
- IPC Health will take all reasonable steps to ensure that the recipient of sensitive information sent outside Victoria will not hold, use or disclose the information other than in accordance with IPC Health's own policies and legislative obligations.

- IPC Health may transfer health information about a client to organisations outside Victoria for the purpose of the provision of care or treatment to a client but only:
    - where the client requests the transfer and consents;
    - where it is believed that the recipient organisation is subject to binding privacy obligations they are substantially similar to the ones under which IPC Health operates;
    - where:
        - it is in the client's interests for the transfer; and
        - it is impracticable to obtain the client's consent; and
        - if it were practicable to obtain consent, the individual would be likely to give consent.

4.11 Sensitive Information

- Health records and other sensitive data must only be accessed to the extent that IPC Health's Personnel's duties require them to do so. This may include access to health records, where there is a demonstrated and direct nexus with an employee's duties such as following up the status of a patient who is no longer in that employee's care or for relevant administrative purposes.
- IPC Health employees must not access the sensitive information of colleagues, friends or family members.

4.12 Handling of Unsolicited Personal Information

- IPC Health Personnel must ensure:
    - unsolicited personal information that does not inform Excellent Care or service delivery is either not recorded or destroyed, or if this is not possible, de-identified, or where this is also not possible, treated with the same level of privacy and confidentiality as solicited information.

4.13 Use of Data for Marketing Purposes

- IPC Health must not use or disclose Personal and/or Health Information for marketing and/or fundraising purposes unless explicit consent has been obtained from the individual to use their information in such a way.
- Where a client has consented to receiving marketing and/or fundraising material from IPC Health, they must also be given a clear and simple option to withdraw their consent and no longer receive marketing and/or fundraising communication from IPC Health.
- IPC Health must ensure any marketing and/or fundraising material is immediately discontinued where an individual has withdrawn their consent and 'opted out' of such material.
- Where an individual has consented to receive marketing and/or fundraising material, IPC Health may provide multiple options to individuals around the type of information they may be contacted about and frequency of contact.

4.14 Making information available to another health provider

- IPC Health must provide a copy or written summary of an individual's Health Information to another health service provider if the individual requests it or if the individual has authorised the other health service provider to request it on their behalf.

Refer to the **Request to Access Information – Client Records Procedure**.

4.15 Transfer or Closure of Service

- In the event of IPC Health being sold or transferred without IPC Health continuing to provide services or if IPC Health is closed down, IPC Health will:
    - publish a notice to that effect in a newspaper circulating in the area in which the business operated; and

- give notice of the transfer or closure to current and past service users, where possible.

4.16 Use of Artificial Intelligence

Artificial intelligence (**AI**) is the simulation of human intelligence processes by computer systems. It involves the development of algorithms, models, and systems enabling machines to perform tasks which typically require human cognitive abilities. IPC Health follows the Department of Health's guidance on the use of unregulated Artificial Intelligence and the use of unregulated generative software such as ChatGPT and other for any clinical purposes.

This includes for:

- clinical applications of generative AI, such as the generation of discharge summaries
- clinical support functions that use generative AI, such as generation of summaries from patient notes and/or patient management system records
- consumer support functions, such as conversational triage 'bots'
- integration of generative AI into clinical services, such as talk-to-text summaries and/or translations, post consultation, unless approved for use e.g. Dragon for transcription services.

A copy of the Department of Health's guidance can be accessed via this link:
https://consultations.health.gov.au/medicare-benefits-and-digital-health-division/safe-and-responsible-artificial-intelligence-in-he/

Under no circumstances should client identifying information be entered into any AI tools unless their use has been appropriately approved for clinical use such as Dragon for transcription services.
Refer to the **IPC Health Artificial Intelligence Policy**.

4.17 Complaints

- IPC Health has an established process for receiving and managing complaints as outlined in the **Client Feedback Procedure**.
- All feedback and complaints regarding privacy matters are be directed to the IPC Health Privacy Officer in the first instance.
- Any individual or their authorised representative may make a complaint regarding a breach of privacy in relation to personal information or an interference with the privacy of an individual in relation to health information.
- A breach of privacy or interference with Health Information Privacy may occur where IPC Health has acted contrary to or inconsistently with the APPs or the HPPs. Examples of an interference with the Apps or HPPs may include:
  - failure to provide access to a client's Health Information.
  - using or disclosing Personal and or Health Information contrary to the APPs or HPPs.
- All complaints must be in writing. Clients will be offered assistance to complete the complaints form if requested.
- The client or their representative should be encouraged to discuss their concerns and resolve the complaint directly with IPC Health.
- The client has the right to have their complaint investigated by the Health Complaints Commissioner or the Privacy Commissioner and information on how to contact these agencies should be made available to the client or their authorised representative.

4.18 Privacy & Confidentiality breaches

- All incidents involving the inappropriate collection, recording, storage, use or release of personal and sensitive information must be notified to the Privacy Officer and entered on the IPC Health incident register

- incidents must be investigated by the relevant management representative or as directed by the Privacy Officer.

- Improper or unauthorised use of personal and sensitive information may be considered as serious misconduct and subject to disciplinary procedures. Privacy related incidents are monitored by the Board Clinical Governance & Clinical Risk Committee and Executive.
- All privacy breach incidents are to be reported to the Privacy Officer, Manager Governance, Quality & Risk (GQR) and Manager and entered in the incident management system.

5. Roles and Responsibilities

5.1 Board of Directors

Monitoring and oversight of privacy practice, ensuring compliance with relevant legislation

5.2 Chief Executive Officer

- Ensuring the principles of this policy and underpinning legislation are applied in the workplace
- Approve document content

5.3 General Manager Financial and Corporate Services

Ensure all information systems, such as network infrastructure and record management systems, are kept secure and functional.

5.4 Governance, Quality and Risk Manager

- Responsible for reporting notifiable data breaches to the Office of the Australian Information Commission (OAIC).
- Provides support to the Privacy Officer functions.
- Support the implementation of improvements to address privacy breaches.
- Maintain a notifiable data breach register.

5.5 Managers

- Responsible for content and implementation.
- Providing support and accountability for privacy practice within their program areas.
- Establishing practice within their respective program areas around collection, storage, use, disclosure, archiving and destruction of personal and sensitive information.

5.6 Privacy Officer (Currently CEO)

- Overall responsibility for ensuring the Client's Health information is maintained appropriately and in accordance with this Policy and all Relevant Privacy Laws.
- Provides advice and support to the organisation around privacy matters, as well as potential and actual privacy related incidents.
- Receives privacy related client feedback or complaints
- Triage privacy and information requests sent through the privacy.officer@ipchealth.com.au e-mail inbox
- Support program and service areas with responding to client information requests and subpoenas.

5.7 All IPC Health Staff

- Are responsible for maintaining privacy, confidentiality and security of any information in IPC Health's possession, and for understanding their obligations and responsibilities under this Policy.

- Ensuring all information, particularly personal, sensitive and/or health information is kept private and secure at all times.
- Only access personal and sensitive information as require to undertake their duties as and employee, volunteer, student or contractor of IPC Heath
- Ensure information on the client health record is kept up to date, accurate and complete.

6. Associated IPC Health frameworks, policies, procedures and guidelines

Advocacy Procedure
Client Information Management Procedure
Clients Rights & Responsibilities Policy
Appropriate Workplace Behaviour Policy
Consent Policy
Court Reports, Subpoenas & Appearance Procedure
Duty of Care – Dignity of Risk Procedure
Ethical Decision Making Procedure
IT Hardware, Software & Business Systems Policy
IT Knowledge & Information Management Policy
ICT Governance Policy
Interpreting and Translating Procedure
Open Disclosure Procedure
Orientation, Induction and Probation Procedure
Request to Access Information – Client Information Procedure
Mobile Devices & BYOD Policy
Privacy and Confidentiality Policy
Data Breaches Procedure
Artificial Intelligence (AI) Policy
Client Feedback Procedure

7. Associated Forms

Consent for Receiving and Sharing information form
Request to Access and Transfer Client Information from IPC Health

8. Associated legislation and other frameworks/guidelines

Health Records Act 2001 (Vic)
Public Records Act 1973 (Vic)
Public Records Vic Disposal Schedule 1999
Privacy and Data Protection Act 2014 (Vic)
Privacy Act 1988 (Cth)
Australian Charter of Healthcare Rights
Family Violence Protection Act 2008 (Vic)
Child Information Sharing Scheme
Family Violence Information Sharing Scheme
Child Wellbeing and Safety Act 2005 (Vic)
Children Youth and Families Act 2005 (Vic)
Child Safe Standards

9. References

Western Region Cross Alliance partner Care Partnerships – DIY Privacy for Primary Care Agencies.
Health Privacy Principles