Australian Chiropractic College

HEALTH PRIVACY

Policy and Procedure

DEFINITIONS

Terms in this document, for which definitions are not provided in the text or may not be self-evident or for which usage at ACC may differ to that in other higher education institutions are as follows:

ACA: Australian Chiropractors Association, which provides a Code of Ethics

AHPRA: Australian Health Practitioner Regulation Agency, which, through the CBA registers for professional practice, suitably qualified graduates of accredited Chiropractic programs.

APP: Australian Privacy Principles, embedded in the Privacy Act (1988).

Chiropractic Board of Australia (CBA): The statutory body responsible for regulating the chiropractic profession in Australia, including registration standards and public protection, and for appointing the CCEA as the accreditation authority for chiropractic education programs.

Chiropractic Centre: A Service Learning Environment provided by the College, either directly or through a relationship with a third-party authorised by the College, for the provision of chiropractic care by Student Interns under the supervision of Chiropractic Supervisors.

Chiropractic Supervisor: Chiropractors who are contracted or otherwise authorised to supervise and/or assess ACC students woth the College's SLEs and WIL environments. In particular within the College's Chiropractic Centres.

Council of Chiropractic Education Australasia (CCEA): The independent accreditation authority appointed by the Chiropractic Board of Australia to accredit and monitor chiropractic education programs, ensuring they meet nationally defined standards for quality, safety, governance, curriculum, resourcing, and graduate competence.

Cultural Safety: Commonly understood as 'an environment that is spiritually, socially and emotionally safe, as well as physically safe for people; where there is no assault challenge or denial of their identity, of who they are and what they need. It is about shared respect, shared meaning, shared knowledge, and experience of learning together' (Williams, 1999 pg. 213). Refer to the College's *Cultural Safety Policy* and *Cultural Safety Procedure.*

Health Privacy: Refers to the ethical and legal obligations governing the collection, use, storage, access, and disclosure of personal and health information within the healthcare context. It encompasses all information arising from the client–practitioner relationship, including clinical records (paper and electronic), health histories, communications, test results, prescribed treatments, and any other identifiable personal data. Health privacy requires practitioners to exercise professional discretion, ensure cultural respect and safety, maintain information security, and obtain informed client consent for access or disclosure to other health practitioners, except where otherwise authorised or required by law. In Australia, health privacy is governed by the *Privacy Act 1988* and *Privacy Amendment Act 2017*, including the Australian Privacy Principles (APPs).

Informed consent: "A person's decision, given voluntarily, to agree to a healthcare treatment, procedure or other intervention that is made, following the provision of accurate and relevant information about the healthcare intervention and alternative options available, and with adequate knowledge and understanding of

the benefits and material risks of the proposed intervention relevant to the person who would be having the treatment, procedure or other intervention." (Australian Commission on Safety and Quality in Health Care, n.d.).

Person Responsible/Responsible Person: An individual who is authorised to make healthcare and health-privacy decisions on behalf of a client who lacks decision-making capacity. This includes, where applicable, a parent of a minor client, a legal guardian, or another individual with lawful authority or recognised standing to act on the client's behalf, derived from applicable legislation, court or tribunal appointment, enduring power of attorney, or accepted clinical and ethical decision-making hierarchies. Such authority is exercised only where the client lacks decision-making capacity and no higher-order directive or instruction of which the College is aware applies.

Privacy Act 1988 (Privacy Act): The primary Australian legislation regulating the collection, use, storage and disclosure of personal information in the private sector and federal public sector. The Privacy Act seeks to give effect to the fundamental right to privacy in Australian society by preventing individuals from being subject to arbitrary interferences with their personal information and protecting them from harm stemming from the misuse of their personal information.

My Health Records Act 2012: The My Health Records Act 2012, establishes the My Health Record system. The My Health Record system contains online summaries of individual's health information which can be viewed by those registered healthcare providers providing care for an individual, including doctors, nurses and pharmacists across Australia.

Service Learning Environments (SLEs)/Contexts/Organisations: An ACC Chiropractic Centre or other Chiropractic practicum/WIL environment where students, under the guidance of Chiropractic or other authorised health professional supervisors, develop their knowledge and skills in Chiropractic practice.

Work Integrated Learning (WIL): "any arrangement where students undertake learning in a work context as part of their course requirements. WIL can be undertaken as part of coursework or research training." (Tertiary Education Quality and Standards Agency, 2022) WIL activities may include: professional workplace placements (also known as internships, Chiropractic placements, fieldwork, practicums) whether local, interstate or international, online or virtual WIL (e.g. telehealth) with real clients or industry input, industry-partnered projects in the classroom that involve industry, community or professional partners, a simulated work environment with industry input, consultation or assessment, or activities in other contexts involving industry or community partners.' May also be synonymous with 'Service Learning'.

PURPOSE

This Health Privacy Policy and Procedure constitutes the ACC's Health Privacy Management Framework and sets out the governance, responsibilities, and procedures through which the College meets its obligations in relation to the handling of personal and health information.

This Policy and Procedure is supplementary to the *ACC Privacy Policy and Procedure*. It outlines the College's commitment to ensuring that all health practitioners and students within its SLEs understand and comply with their obligations under the *Privacy Act 1988*, the *Privacy Amendment Act 2000*, (which amends the Privacy Act for the Private Sector), the *Australian Privacy Principles* (APP) set out in the Privacy Act, and the *APP Guidelines, 2019*, with respect to **Health Privacy** requirements.

In addition to the relevant Acts and to the ACC's overarching *Privacy Policy and Procedure*, this document is to be read in conjunction with the AHPRA *Shared Code of Conduct* adopted by the Chiropractic Board of Australia, and ACC expectations and rules for various aspects of professional ethics and conduct, as outlined in the policies and procedures of the College that are listed under *Related Policy Documents* below.

The *Health Privacy Policy and Procedure* is also aligned with the requirements inherent in HESF (2021), specifically:

- 3. Teaching (3.1 Course Design: 3.1.3)
- 5. Institutional Quality Assurance (5.4 Delivery with Other parties: 5.4.1, 5.4.2)
- 6. Governance and Accountability (6.2 Corporate Monitoring and Accountability: 6.2.1 (a); 6.3 Academic Governance: 6.3.1 (a),(c),(d)
- 7. Representation, Information and Information Management (7.2 Information or Current and Prospective Students:7.2.2 (c),(d).

Furthermore, it aligns with the CCEA's *Accreditation Standards for Chiropractic Programs and Competency Standards for Chiropractors* (2025), specifically:

- **Standard 1: Public Safety** (Criteria 1.1, 1.2, 1.3, 1.4, 1.5, **1.6, 1.7, 1.8, 1.9**)
- **Standard 2: Governance and quality improvement** (Critereon 2.6 a.)
- **Standard 3: Program of Study** (Criteria 3.5, 3.8, 3.10)
- **Standard 6: Cultural Safety** (**Criteria 6.1, 6.4, 6.6, 6.10**)
- **Universal Competency 1: Practising Professionally** (Criteria 1.1, 1.2, 1.4, 1.5)
- **Universal Competency 2: Practising in a culturally safe and respectful way** (**Criteria 2.1, 2.2, 2.3**)
- **Universal Competency 3: Communication, Collaboration and Leadership** (Criteria 3.1, 3.2, 3.3)
- **Practice Competency 4: Clinical Assessment** (Criteria 4.1, 4.2, 4.3, 4.4, 4.5)
- **Practice Competency 5: Planning Care** (Criteria 5.1, 5.2, 5.3)
- **Practice Competency 6: Implementing, Monitoring and Evaluating Care** (Criteria 6.1, 6.2, 6.3, 6.4)

The ACC requires that all staff (employed or contracted) and students, including those engaged in SLEs and/or WIL, are proactive in establishing, implementing and maintaining health privacy processes in accordance with this Policy and Procedure.

Any breach of the ACC's requirements for compliance with expectations for the health privacy of clients may result in penalties, sanctions or other disciplinary action in accordance with ACC Code of Conduct and other relevant ACC Policies and Procedures as listed under *Related Policy Documents* below.

In addition, the ACC requires that all staff (employed or contracted) and students engaged in SLEs and/or WIL are familiar with the concept of Cultural Safety as defined above, and requires that they foster Cultural Safety in all ACC contexts, including the ACC Chiropractic Centres and other SLEs.

SCOPE

This Policy applies to all staff, contractors, and enrolled students, and covers all learning and teaching activities and settings, whether on- or off-campus. This includes scheduled classes, 'Outreach' Chiropractic Centres, and approved extra-curricular activities.

POLICY

1. Background

In Australia, private sector health service providers are subject to the Privacy Act. The Privacy Act applies nationwide to private health services regardless of location, and in New South Wales, Victoria and the Australian Capital Territory (ACT) these private providers must comply with both the Privacy Act and applicable state or territory privacy laws when handling health information. In Queensland, the Northern Territory and Tasmania, there is privacy legislation that primarily applies to public sector agencies; private sector health providers in those jurisdictions remain governed by the Privacy Act. In Western Australia, the Privacy and Responsible Information Sharing Act 2024 comes into effect on 1st July 2026, which will establish a public sector privacy framework. South Australia currently does not have a standalone health privacy statute but has privacy principles for government agencies. This layered framework means health privacy obligations derive from a combination of federal and, where relevant, state or territory privacy regimes.

Whilst ACC staff, students, contractors and associates are primarily involved in SLEs/WIL activities in ACC Chiropractic Centre/s and other contexts in South Australia and Victoria, they are required to familiarise themselves with Health Privacy Law and Policies and Procedures applicable to health contexts interstate or overseas if they undertake WIL in such locations.

2. Institutional Commitment

The ACC is committed to providing safe, respectful, and professionally appropriate learning environments in which standards of conduct and behaviour are of the highest order. As part of their education, students develop clinical knowledge and skills through clinical practicum and WIL undertaken within a range of supervised simulated and SLEs, where health privacy obligations apply.

Accordingly, the ACC is committed to upholding the principles and obligations of the Privacy Act 1988 (Cth), including the Australian Privacy Principles (APPs), as reflected in the College's Privacy Policy and associated procedures. These principles guide the lawful, ethical, and respectful handling of health information across all ACC clinical and service learning activities.

This Health Privacy Policy is informed by the Health Privacy Guide (Office of the Australian Information Commissioner, 2019), which provides guidance to health service providers in meeting their obligations under the Privacy Act 1988 and the Australian Privacy Principles.

Through its clinical and service learning activities, the ACC provides healthcare services to a diverse range of clients. The provision of safe and effective care necessarily involves the collection and use of health information relevant to assessment, treatment, education, and continuity of care.

The ACC is committed to ensuring that all health information is treated as confidential and is managed in a manner that protects client privacy and dignity. Health information will only be accessed, used, or disclosed in accordance with applicable privacy legislation, ethical standards, and informed consent, except where otherwise permitted or required by law.

The ACC also recognises the rights of individuals to access and seek correction of their health information in accordance with applicable privacy legislation and College policies. Detailed processes for the management, access, and disclosure of health information are set out in the associated Health Privacy Procedures and Health Privacy Management Framework.

RELATIONSHIP OF THE HEALTH PRIVACY POLICY AND PROCEDURE TO THE ACC PRIVACY POLICY AND PROCEDURE

The ACC *Privacy Policy and Procedure* outlines the College processes related to the collection of personal information for the purposes of all of the activities undertaken by the College. The *Health Privacy Policy and Procedure* provides further detailed information on considerations and obligations relevant to health-related personal data.

Delegation of Health Privacy Responsibilities

The ACC retains overall responsibility and accountability for compliance with health privacy obligations in accordance with this Health Privacy Policy and Procedure and applicable legislation.

The College may delegate operational responsibilities for the handling of personal and health information to authorised staff members, contractors, and partner organisations acting on behalf of the College, including within clinical education and service learning contexts. Any such delegation is subject to this Policy and Procedure and does not diminish the College's overarching responsibility for health privacy governance and compliance.

Roles, responsibilities, and reporting arrangements relating to delegated health privacy functions are set out in the Procedures section of this document and in relevant contractual and governance instruments.

HEALTH PRIVACY MANAGEMENT FRAMEWORK – POLICY

The main principles of the ACC Health Privacy Management Framework to which ACC is committed are:

a. Embedding a culture of privacy that enables compliance with relevant statutory and ethical obligations.
b. Establishing robust and effective privacy processes.
c. Fostering Cultural Safety as an integral element of the College's Health Privacy Policy and Procedures.
d. Monitoring and reviewing privacy processes to ensure continued effectiveness.
e. Continuous improvement of the College's management capability and proactive response to privacy issues that may arise.

This is evidenced in the following:

Designated Health Privacy Officer

The ACC designates a Health Privacy Officer with institutional responsibility for oversight of health privacy governance within the College.The Health Privacy Officer is responsible for supporting the College's compliance with the *Privacy Act 1988* (Cth), the Australian Privacy Principles (APPs), and this Health Privacy Policy and Procedure, including providing authoritative advice on the handling of health information within the SLEs and WIL contexts.

In particular, the Health Privacy Officer has responsibility for:

- providing guidance to staff and students on health privacy obligations and the application of this Policy in clinical and service learning environments;
- supporting the identification, management, and escalation of health privacy risks and incidents, including data breaches, in accordance with College procedures;
- acting as a central point of coordination for privacy-related complaints, queries, and compliance matters arising within SLE and WIL contexts; and
- contributing to institutional monitoring, review, and continuous improvement of health privacy practices.

The designated Health Privacy Officer for the purposes of this Policy is the Program Coordinator, Chiropractic Sciences, who exercises this role within the College's broader governance, quality assurance, and risk management frameworks.

Documented Oversight of Health Information

The ACC requires the maintenance of documented oversight of the personal and health information handled by staff and students engaged in Health Practicum and Work Integrated Learning (WIL) environments. This oversight forms part of the College's governance framework for ensuring compliance with the *Privacy Act 1988* (Cth), the Australian Privacy Principles (APPs), and relevant accreditation and quality assurance requirements. Accordingly, the College maintains a documented record that identifies, at a minimum:

- the categories of personal and health information handled within ACC Chiropractic Centres and associated Service Learning Environments, including clinical records and other information arising from the client–practitioner relationship;
- the primary sources and pathways through which such information is collected or received in the course of clinical education and service delivery; and
- the locations and forms in which personal and health information is held, including physical and electronic records and any use of external or cloud-based storage arrangements.

This documentation supports the College's ability to manage privacy risks, safeguard health information, ensure accountability across multiple clinical and service learning contexts, and meet its obligations under applicable privacy legislation and regulatory standards.

Staff and Student Training

The ACC requires that all staff, contractors, and enrolled students whose roles involve the handling of personal or health information receive appropriate and ongoing training in health privacy obligations.

Such training supports the College's compliance with the Privacy Act 1988 (Cth), the Australian Privacy Principles (APPs), and this Health Privacy Policy and Procedure, and is intended to ensure that personal and health information is managed lawfully, ethically, securely, and with due regard for Cultural Safety across all College activities.

Health privacy training must ensure that staff and students have an appropriate understanding of:

- the nature and sensitivity of personal and health information handled by the College;
- their responsibilities and obligations in relation to the collection, use, storage, access, and disclosure of health information;
- the application of informed consent and authorised decision-making in health and health-privacy contexts;
- privacy risks, including data breaches, and the importance of timely identification and escalation of such risks; and
- the specific privacy considerations that arise in clinical education, including within SLE and WIL contexts, where applicable.

The College maintains oversight of health privacy training as part of its governance and quality assurance framework to support consistent compliance and continuous improvement.

Publication of the College's Health Privacy Policy and Procedure

The ACC is committed to openness and transparency in the management of personal and health information.

The College ensures that its Health Privacy Policy and Procedure is publicly available and accessible, and that individuals are able to obtain information about how their personal and health information is collected, used, stored, and disclosed by the College, in accordance with the *Privacy Act 1988* (Cth) and the Australian Privacy Principles (APPs).

The College further commits to making information about health privacy available in a manner that supports informed understanding and trust, having regard to the contexts in which health information is handled and the needs of individuals whose information is collected.

Protection and Security of Health Information

The ACC is committed to protecting personal and health information from misuse, interference, loss, and from unauthorised access, modification, or disclosure, in accordance with the Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs).

The College maintains documented governance arrangements that support the protection and security of health information across all College activities, including those involving clinical education and service delivery. These arrangements provide for the identification and management of privacy and information security risks, and support compliance with relevant legislative, regulatory, and accreditation requirements.

The College requires that appropriate processes and safeguards are in place to ensure that personal and health information is managed securely throughout its lifecycle, including collection, storage, use, disclosure, and disposal, in accordance with applicable policies and procedures.

Data Breach Management

The ACC recognises that data breaches involving personal or health information may occur and is committed to responding to such incidents promptly, appropriately, and in accordance with applicable legal and regulatory requirements.

The College maintains arrangements to ensure that actual or suspected data breaches are identified, assessed, managed, and, where required, notified in compliance with the Privacy Act 1988 (Cth), the Australian Privacy Principles (APPs), and the Notifiable Data Breaches scheme.

The ACC requires that data breaches are managed in a manner that prioritises the protection of individuals from harm, supports transparency and accountability, and enables continuous improvement of the College's privacy and information security practices.

Detailed responsibilities, reporting pathways, and response processes are set out in the Procedures section of this document and related governance documents.

Health Privacy Risk Identification and Management

The ACC is committed to the proactive identification, assessment, and management of risks associated with the handling of personal and health information across all College activities.

Health privacy risks are recognised as a component of the College's broader risk management and governance framework. The College requires that risks relating to health privacy are identified, reported, and addressed in a timely manner to support compliance with legal obligations, protect individuals from harm, and maintain trust in the College's educational and clinical activities.

The ACC promotes a culture of accountability and transparency in which staff, contractors, and students are expected to raise health privacy risks or concerns through established College governance and reporting mechanisms.

Processes for risk identification, escalation, monitoring, and review are set out in the Procedures section of this document and associated procedures.

HEALTH PRIVACY MANAGEMERNT FRAMEWORK - PROCEDURES:

1. Collection of Information

Personal and health information may only be collected by the College where it is reasonably necessary for the provision of healthcare services, clinical education, supervision, continuity of care, or to meet legal, professional, or accreditation requirements.

1.1 Authorisation to collect information

Personal and health information may be collected only by:

- registered health practitioners engaged by or on behalf of the College;
- ACC staff acting within the scope of their role; or
- students undertaking clinical or service learning activities under appropriate supervision.

Students must not independently determine the scope, method, or purpose of information collection and must collect information only in accordance with supervisory direction and this Procedure.

1.2 Limitation and necessity

The collection of personal and health information must be limited to information that is reasonably necessary for the identified purpose. Information that is not relevant to clinical care, education, supervision, or legal obligations must not be collected.

1.3 Client awareness at the point of collection

At or before the time personal or health information is collected, reasonable steps must be taken to ensure that clients are aware of:

- who is collecting the information;
- the general purpose for which the information is being collected; and
- the involvement of students in care or information handling, where applicable.

This requirement applies regardless of whether formal written consent is obtained at a later stage.

1.4 Cultural Safety and voluntariness

Information must be collected in a manner that is fair, respectful, non-coercive, and culturally safe. Clients must be afforded dignity and respect throughout the collection process and may decline to answer particular questions without prejudice to their care, except where the information is essential for safe and lawful practice.

1.5 Collection from third parties

Personal or health information about a client may be collected from third parties (including family members, other health practitioners, insurers, or legal representatives) only where:

- the client or their authorised Responsible Person has consented; or
- the collection is authorised or required by law.

Information collected from third parties must be relevant to the stated purpose and handled in accordance with this Policy and Procedure.

1.6 Audio, visual, and digital recording

The collection of personal or health information by way of audio recording, video recording, photography, or other digital media requires explicit and informed consent specific to that form of collection. Such consent must not be assumed to be included within general intake or treatment consent.
Clients may refuse audio, visual, or digital recording without impact on their access to care.

1.7 Recording standards

Personal and health information recorded at the point of collection must be accurate, objective, relevant, and professionally appropriate. Records must be created in a manner consistent with professional standards and are subject to review and oversight within the College's supervisory and governance arrangements.

1.8 Relationship to other procedures

The collection of personal and health information under this section must be read in conjunction with the Procedures relating to consent, use and disclosure, data security, access and correction, and data breach management set out in this document.

1.9 Collection and use of health information for research purposes

The College may collect, use, or disclose personal or health information for the purposes of research only where such activity has received prior approval from an appropriately constituted Human Research Ethics Committee (HREC) or other recognised ethics approval body.

All research involving human participants, including the collection or use of personal or health information, must be conducted in accordance with the *Privacy Act 1988* (Cth), the Australian Privacy Principles (APPs), and the "National Statement on Ethical Conduct in Human Research" issued by the National Health and Medical Research Council (2023).

Where health information is collected or used for research purposes:

- the information must be limited to what is necessary to achieve the approved research objectives;
- informed consent must be obtained from participants unless a waiver of consent has been approved by the relevant ethics committee in accordance with the National Statement;
- personal and health information must be handled in accordance with the conditions of the ethics approval, including requirements relating to confidentiality, data security, retention, and destruction or de-identification; and
- the involvement of students in research activities must occur under appropriate supervision and strictly within the scope of the approved ethics protocol.

No research activity involving personal or health information may commence until all required ethics approvals have been obtained.

2. Consent:

Consent is required for the collection, use, and disclosure of personal and health information, except where otherwise authorised or required by law.

Consent under this section relates specifically to decisions about the handling of personal and health information. It is distinct from informed consent to receive healthcare treatment, which is addressed in the ACC Informed Consent Policy and Procedure.

2.1 Responsibility for obtaining consent

Consent for the handling of personal and health information must be obtained within an appropriately supervised clinical or service learning context.

Where students are involved in care or information handling, consent is obtained under the authority and oversight of a supervising practitioner or authorised ACC staff member. Students must not independently determine the adequacy or scope of consent.

2.2 Information to be provided when seeking consent

Before consent is obtained, reasonable steps must be taken to ensure that the client is informed of:

- the purpose for which their personal or health information is being collected, used, or disclosed;
- the identity of the relevant ACC Chiropractic Centre or Service Learning Environment;
- the involvement of students in care or information handling, where applicable;
- their right to access and seek correction of their health information; and
- the potential consequences of not providing required information, including any impact on the provision of services.

Information must be provided in a manner that is clear, culturally safe, and appropriate to the client's capacity and circumstances.

2.3 Forms of consent

Consent may be express or implied, depending on the circumstances.

- **Express consent** is given explicitly, either orally or in writing, through a clear and voluntary affirmative act.
- **Implied consent** may arise where, having regard to the circumstances and the conduct of the client, it is reasonable to infer that consent has been given.

Written consent is required where:

- personal or health information is to be disclosed to another health service provider or third party;
- audio, visual, or digital recording is proposed; or
- consent is otherwise required by College procedures or law.

2.4 Voluntariness and withdrawal of consent

Consent must be given voluntarily and without coercion.

Clients may refuse to provide consent, or may withdraw or limit consent, in whole or in part, at any time. Where consent is refused or withdrawn, reasonable steps must be taken to explain any consequences for care or service provision, and such refusal or withdrawal must not result in unfair treatment or discrimination.

Any withdrawal or limitation of consent must be appropriately documented.

2.5 Capacity and Responsible Persons

Where a client lacks decision-making capacity, consent for the handling of personal or health information may be provided by an authorised Responsible Person in accordance with applicable law and this Policy and Procedure.

Where personal or health information is collected from a Responsible Person rather than directly from the client, reasonable steps must be taken to ensure that the client is informed of this, where appropriate.

2.6 Consent in research contexts

Where personal or health information is collected or used for research purposes, consent requirements are governed by the approved ethics protocol and must be consistent with the *Privacy Act 1988* (Cth), the Australian Privacy Principles (APPs), and the National Statement on Ethical Conduct in Human Research (2023).

Consent waivers approved by a Human Research Ethics Committee apply only within the scope of the approved research and do not override consent requirements for clinical care or other College activities.

3. Use & Disclosure of Personal and Health information

Personal and health information collected by the College must only be used or disclosed for lawful and authorised purposes in accordance with this Policy and Procedure.

3.1 Primary purpose

Personal and health information may be used or disclosed for the primary purpose for which it was collected, including the provision of healthcare services, clinical education, supervision, continuity of care, and related administrative functions, where such use or disclosure is reasonably necessary.

3.2 Secondary purposes

Personal or health information must not be used or disclosed for a secondary purpose unless:

- the secondary purpose is directly related to the primary purpose, and the individual would reasonably expect the use or disclosure; or
- the client or their authorised Responsible Person has provided consent; or
- the use or disclosure is authorised or required by law.

Secondary use or disclosure for direct marketing purposes is not permitted.

3.3 Authorisation and supervision

Decisions regarding the use or disclosure of personal and health information must be made by authorised ACC staff or supervising practitioners.

Students must not independently authorise or initiate disclosures of personal or health information and may only participate in such activities under appropriate supervision and in accordance with this Procedure.

3.4 Disclosure to other health service providers

Personal or health information may be disclosed to another health service provider where:

- the disclosure is necessary for the provision or continuity of care; and
- the client or their authorised Responsible Person has provided consent, unless disclosure is otherwise authorised or required by law.

Written consent is required where disclosure occurs outside routine clinical referral or handover processes.

3.5 Disclosure to Responsible Persons

Personal or health information may be disclosed to a Responsible Person where:

- the client lacks decision-making capacity or is unable to communicate consent; and
- the disclosure is necessary for appropriate care or treatment, or is made for compassionate reasons; and
- the disclosure is not contrary to any known wishes previously expressed by the client.

3.6 Research-related use and disclosure

Personal or health information may only be used or disclosed for research purposes where such use or disclosure is within the scope of an approved ethics protocol and in accordance with the *Privacy Act 1988* (Cth), the Australian Privacy Principles (APPs), and the National Statement on Ethical Conduct in Human Research (2023).

Research-related use or disclosure must not occur unless all required ethics approvals have been obtained.

3.7 Emergency and serious threat disclosures

Personal or health information may be used or disclosed without consent where the use or disclosure is reasonably necessary to prevent or lessen a serious and imminent threat to the life, health, or safety of the client or another individual, and where it is not practicable to obtain consent.

3.8 Use and disclosure for audit, accreditation, and quality assurance

Personal and health information may be used or disclosed for the purposes of audit, accreditation, quality assurance, and internal monitoring and evaluation where such use or disclosure is reasonably necessary to support the College's governance, regulatory, and educational obligations.

This includes, but is not limited to:

- internal audits and quality assurance activities;
- clinical record audits conducted as part of accreditation or regulatory review processes, including those undertaken by the CCEA; and
- the extraction and analysis of data for internal reporting, evaluation, and continuous improvement.

Use or disclosure under this section must be:

- limited to the minimum information necessary to achieve the stated purpose;
- conducted using de-identified or aggregated information where practicable;
- restricted to authorised individuals or bodies subject to confidentiality obligations; and
- documented in a manner sufficient to support accountability and review.

Use or disclosure of personal or health information under this section must not be undertaken for marketing or other unrelated secondary purposes.

3.9 Documentation of use and disclosure

Any use or disclosure of personal or health information other than for the primary purpose must be appropriately documented, including:

- the purpose of the use or disclosure;
- the authority relied upon (e.g. consent, legal requirement, emergency); and
- the parties to whom the information was disclosed.

Documentation must be sufficient to support accountability and review.

4. Data Accuracy and Quality

The College must take reasonable steps to ensure that personal and health information it collects, uses, or discloses is accurate, complete, relevant, and up to date.

4.1 Accuracy at the point of collection

Personal and health information must be recorded accurately and objectively at the time of collection. Information recorded by students must be subject to appropriate review and oversight by supervising practitioners or authorised ACC staff.

4.2 Ongoing accuracy

Where personal or health information is used or disclosed, reasonable steps must be taken to ensure that the information is current and relevant to the purpose for which it is being used or disclosed.

Information that is known, or reasonably suspected, to be inaccurate, incomplete, or out of date must not be relied upon where this could reasonably be expected to affect clinical care, decision-making, or other authorised purposes.

4.3 Identification and correction of errors

Where an error or inaccuracy in personal or health information is identified by staff, students, or supervising practitioners, reasonable steps must be taken to correct the information or to record the correct information in accordance with the Procedures relating to access and correction.

Students must report identified inaccuracies to their supervisor and must not independently alter records outside their authorised role.

4.4 Documentation

Corrections to personal or health information must be documented in a manner that maintains the integrity of the record and supports transparency and accountability.

5. Data security

The College must take reasonable steps to protect personal and health information from misuse, interference, loss, and from unauthorised access, modification, or disclosure.

5.1 Responsibility for data security

All staff, contractors, and students who handle personal or health information are responsible for maintaining the security and confidentiality of that information in accordance with this Policy and Procedure and other relevant College policies.

Students must access and handle personal and health information only under appropriate supervision and within the scope of their authorised learning activities.

5.2 Access controls

Access to personal and health information must be restricted to authorised individuals on a need-to-know basis.

Reasonable steps must be taken to ensure that:

- access rights reflect current roles and responsibilities;
- unauthorised access is prevented; and
- access is reviewed and adjusted where roles change.

5.3 Physical and electronic security

Personal and health information must be stored securely, whether in physical or electronic form.

Reasonable security measures must be applied to protect information against unauthorised access, loss, or damage, including during storage, transmission, and use.

5.4 Use of systems, devices, and locations

Personal and health information must only be accessed, stored, or transmitted using systems, devices, and locations authorised by the College.

The use of personal devices or unauthorised systems to store or transmit personal or health information is not permitted unless expressly authorised under College policy. Personal devices may be authorised by the College under a Bring Your Own Device (BYOD) arrangement, subject to compliance with specified security requirements.

Clinical supervisors are responsible for ensuring student interns comply with BYOD requirements and to provide ongoing reminders of compliance requirements.

5.5 Third-party and service provider arrangements

Where personal or health information is handled by third parties, including contracted Service Learning Environments or cloud service providers, reasonable steps must be taken to ensure that such handling is subject to appropriate security, confidentiality, and privacy obligations consistent with this Policy and Procedure.

5.6 Retention, destruction, and de-identification

Personal and health information must be retained only for as long as required for lawful and authorised purposes.

When personal or health information is no longer required, reasonable steps must be taken to ensure that the information is securely destroyed or permanently de-identified in accordance with applicable College policies and legal requirements.

5.7 Relationship to data breach management

Any actual or suspected compromise of the security of personal or health information must be managed in accordance with the data breach procedures set out in this document.

6. Openness

The College must ensure that individuals are able to readily obtain clear and accurate information about how their personal and health information is managed.

6.1 Availability of health privacy information

The Health Privacy Policy and Procedure must be made available in a manner that supports openness, transparency, and informed understanding, in accordance with the *Privacy Act 1988* (Cth) and the Australian Privacy Principles (APPs).

6.2 Communication with clients

Where personal or health information is collected, reasonable steps must be taken to ensure that clients are informed of the College's health privacy practices, including:

- the kinds of personal and health information collected;
- the purposes for which the information is collected, used, and disclosed;
- how individuals may access and seek correction of their information; and
- how privacy concerns or complaints may be raised.

Information must be provided in a manner that is clear, respectful, and appropriate to the individual's circumstances and capacity.

6.3 Requests for information

Where an individual requests information about the College's health privacy practices, reasonable steps must be taken to respond accurately and in a timely manner, having regard to the nature of the request and the information sought.

6.4 Relationship to other procedures

Procedures relating to consent, access and correction, complaints, and data breach management give effect to the College's commitment to openness and must be applied consistently with this section.

7. Access to Personal and Health Information

Individuals have the right to request access to personal and health information held by the College about them, subject to the limitations set out in this Procedure.

7.1 Making an access request

Requests for access to personal or health information may be made by the client or their authorised Responsible Person.

Reasonable steps must be taken to verify the identity and authority of the person making the request before access is provided.

7.2 Provision of access

Subject to section 7.3, the College must provide access to the requested personal or health information within a reasonable period and in a manner that supports understanding.

Access may be provided by inspection, by providing a copy or summary of the information, or by other reasonable means, having regard to the nature of the information and the request.

7.3 Grounds for refusing or limiting access

Access to personal or health information may be refused or limited where:

- providing access would pose a serious threat to the life, health, or safety of the client or another individual;
- providing access would have an unreasonable impact on the privacy of other individuals;
- the request is frivolous or vexatious;
- the information relates to existing or anticipated legal proceedings between the client and the College and would not otherwise be accessible through legal discovery processes; or
- access is required to be refused by law or authorised enforcement activity.

Where access is refused or limited, reasonable steps must be taken to provide the individual with written reasons for the decision.

7.4 Student records and supervision

Where personal or health information includes material created by students, access decisions must be made with regard to supervision, professional standards, and the integrity of the clinical record.

The involvement of students in record creation does not, of itself, justify refusal of access.

7.5 Fees

The College may charge a reasonable fee for providing access to personal or health information where permitted by law. Any fee must be limited to the cost of providing access and must not be excessive or prohibitive.

No fee may be charged for making an access request.

7.6 Documentation

Access requests, decisions, and any refusals or limitations must be documented in a manner that supports accountability, review, and compliance with this Procedure.

8. Correction of Personal and Health Information

The College must take reasonable steps to ensure that personal and health information it holds is accurate, complete, relevant, and up to date.

8.1 Requests for correction

A client or their authorised Responsible Person may request correction of personal or health information held by the College where they believe the information is inaccurate, incomplete, misleading, or out of date.

Requests for correction may be made regardless of whether the information was originally collected directly from the client or from another source.

8.2 Assessment of correction requests

Upon receiving a request for correction, reasonable steps must be taken to assess the request having regard to:

- the nature of the information;
- the purpose for which the information is held and used; and
- any supporting information provided by the client or Responsible Person.

8.3 Making corrections

Where the College is satisfied that the information is inaccurate, incomplete, misleading, or out of date, the information must be corrected in a timely manner.

Corrections must be made in a way that:

- preserves the integrity of the original record;
- ensures the corrected information is clearly identifiable; and
- supports continuity of care and accountability.

Students must not independently correct records and must refer correction requests to their supervisor or authorised ACC staff member.

8.4 Refusal to correct

Where the College refuses to correct personal or health information as requested, reasonable steps must be taken to provide the client or Responsible Person with written reasons for the refusal.

If requested, reasonable steps must also be taken to associate a statement with the relevant record indicating that the individual considers the information to be inaccurate, incomplete, misleading, or out of date.

8.5 Notification of corrections

Where personal or health information has been corrected, reasonable steps must be taken to notify any other health service provider or third party to whom the information has been disclosed, where appropriate and practicable.

8.6 Documentation

Requests for correction, decisions made, actions taken, and any statements associated with records must be documented in a manner that supports transparency, accountability, and compliance with this Procedure.

9. Sensitive information

For the purposes of this Policy and Procedure, all health information is treated as sensitive information and is subject to heightened privacy protections in accordance with the Privacy Act 1988 (Cth).

10. Release of Health Information

Personal and health information may be made available to or obtained from another health service provider where such disclosure or collection is necessary for the provision of healthcare services, continuity of care, clinical education, or other lawful and authorised purposes.

10.1 Disclosure to another health service provider

The College may disclose personal or health information to another health service provider where:

- the client or their authorised Responsible Person has provided consent; or
- the disclosure is otherwise authorised or required by law.

Disclosure must be limited to information that is reasonably necessary for the stated purpose.

10.2 Collection of information from another health service provider

The College may request or collect personal or health information from another health service provider where:

- the client or their authorised Responsible Person has consented to the collection; or
- the collection is otherwise authorised or required by law.

Information collected must be relevant to the purpose for which it is sought and handled in accordance with this Policy and Procedure.

10.3 Authorisation and supervision

Decisions to disclose or request personal or health information from another health service provider must be made by authorised ACC staff or supervising practitioners.

Students must not independently authorise requests for, or disclosures of, personal or health information to or from another health service provider.

10.4 Documentation

Any disclosure to, or collection from, another health service provider must be documented, including:

- the purpose of the disclosure or collection;
- the authority relied upon (e.g. consent, legal requirement); and
- the identity of the receiving or providing health service provider.

Documentation must be sufficient to support accountability, continuity of care, and audit.

11. Management of Data Breaches

A data breach occurs where personal or health information is lost, accessed, used, disclosed, modified, or otherwise handled in an unauthorised manner.

11.1 Identification and reporting

All staff, contractors, and students must immediately report any actual or suspected data breach involving personal or health information to an authorised supervisor or designated College officer in accordance with this Procedure.

Students must not attempt to investigate, resolve, or contain a suspected data breach independently.

11.2 Escalation and oversight

Any actual or suspected data breach must be promptly escalated to the **Chief Executive Officer (CEO)**, who holds delegated responsibility for the investigation, management, and oversight of data breaches on behalf of the College.

The CEO may seek advice from, or delegate aspects of investigation and response to, appropriately authorised staff or agent, while retaining overall accountability for breach management.

11.3 Assessment and response

Upon notification of a data breach, reasonable steps must be taken to:

- assess the nature and scope of the breach;
- determine the likelihood of serious harm to affected individuals;
- contain the breach and mitigate any ongoing risk; and
- identify corrective actions to prevent recurrence.

11.4 Notification obligations

Where a data breach meets the threshold for notification under the *Privacy Act 1988* (Cth) and the Notifiable Data Breaches scheme, the CEO is responsible for ensuring that:

- the Australian Information Commissioner is notified; and
- affected individuals are notified, where required.

Where the breach involves information held in the My Health Record system, notification obligations under the *My Health Records Act 2012* must also be met.

11.5 Confidentiality and information handling

All information relating to an actual or suspected data breach must be treated as confidential and handled in accordance with this Policy and Procedure.

Information relating to a breach may be disclosed where required for investigation, regulatory reporting, legal proceedings, or law enforcement purposes. Disclosure must be limited to those persons for whom the information is reasonably necessary.

The identity of a person reporting a data breach must be protected as far as practicable, unless disclosure is required by law or is necessary to enable effective investigation or resolution.

11.6 Documentation and review

All data breaches, including near misses, must be documented in a manner that supports accountability, reporting, and review.

The College must use information arising from data breaches to inform continuous improvement of its privacy, information security, and risk management practices.

IMPLEMENTATION and MONITORING

The implementation of this policy and procedure is the responsibility of the Program Coordinator Chiropractic Sciences, under delegated authority from the Academic Dean.

The CEO will report quality assurance, compliance or other issues that arise, as part of the Quality Assurance Cycle, through end of semester reports to the Academic Board. All data breach incidents are reported to by the CEO to the Academic Board, Finance Audit and Risk Committee and the Board of Directors.

The Program Coordinator Chiropractic Sciences will also ensure that all potential risks under, and any breaches of, this Policy and Procedure are notified immediately to the ACC CEO, who will in turn inform the President and Academic Dean.

RELATED LEGISLATION, REGULATORY REQUIREMENTS and REFERENCES

- ACA Code of Ethics https://www.chiro.org.au/wp-content/uploads/2019/12/ACA-code-of-ethics2017.pdf
- AHPRA (Chiropractic Board), June 2022, *Shared - Code of Conduct*.
- *Informed consent.* (n.d.). Australian Commission on Safety and Quality in Health Care. https://www.safetyandquality.gov.au/our-work/partnering-consumers/informed-consent
- *Australian Privacy Principles* (embedded in the Privacy Act 1988) - replaced the National Privacy Principles and Information Privacy Principles March 2014.
- *Accreditation Standards for Chiropractic Programs and Competency Standards for Chiropractors.* (2025). Council on Chiropractic Education Australasia. https://www.ccea.com.au/standards
- *My Health Record Act 2012* (Commonwealth).
- National Health and Medical Research Council (Australia), Australian Research Council & Universities Australia. (2023). *National statement on ethical conduct in human research 2023*. National Health and Medical Research Council. http://nla.gov.au/nla.obj-3260080025
- OAIC (Office of Australian Information Commissioner) 2021, *Guide to securing personal information.*
- OAIC (Office of Australian Information Commissioner) 2019, *Data breach preparation and response - A guide to managing data breaches in accordance with the Privacy Act 1988* (Commonwealth)
- *Privacy Act 1988* (Commonwealth).
- *Privacy Amendment (Enhancing Privacy Protection) Act 2012*, which amends the Privacy Act 1988.
- Tertiary Education Quality and Standards Agency. (2022, May 4). *Guidance note: Work-integrated learning.* Tertiary Education Quality and Standards Agency. https://www.teqsa.gov.au/guides-resources/resources/guidance-notes/guidance-note-work-integrated-learning
- Williams, R. 1999. Cultural Safety - What does it mean for our work practice? *Australian and New Zealand Journal of Public Health,* 23(2). 213-214). Also cited by the South Australia Government, Office

of the Commissioner for Public Sector Employment, *Public Sector Work Health and Safety Framework for Cultural Safety*.

REVIEW

The ACC's Health Privacy Policy and Procedures is reviewed every three years.

It is a policy of the ACC that any Policy or Procedure may be reviewed earlier as indicated by internal or external factors (including but not limited to such factors as changes in the guidelines of regulatory authorities, accreditation/registration requirements of the profession, or relevant legislation at state or federal level) as determined the Board of Directors and/or Academic Board.

RELATED POLICY DOCUMENTS

- Privacy Policy and Procedures
- Cultural Safety Policy
- Cultural Safety Procedure
- WIL/Chiropractic Practicum Framework
- WIL/Chiropractic Practicum Policy
- WIL/Chiropractic Practicum Procedure
- Assessment of Coursework Policy
- Staff Induction and Professional Development Policy and Procedures
- Secure Information Management Policy and Procedures
- Records Management Policy
- Code of Conduct Policy and Procedures
- Grievance Management Non-Academic (Students) Policy and Procedures
- Grievance Management (Staff) Policy and Procedures

VERSION CONTROL

Document: A020 Health Privacy Policy and Procedure		
Responsible Officer: Program Coordinator Chiropractic Sciences, by delegated authority from the Academic Dean		
Initially endorsed by: Academic Board		**Date:** 25 January 2023
Reviewed and Approved by: Academic Board		**Date:** 6 May 2026
HESF	1.4 Learning Outcomes and Assessment	1.4.2b 1.4.2c
Version: V2	**Replaces Version(s)**: V1	**Next Review:** January 2026
Nature of change	**May 2026:** Comprehensive review and restructure of the Health Privacy Policy and Procedure to align with updated privacy legislation, contemporary governance and risk management requirements, and the CCEA Accreditation Standards and Competency Standards (2025). Revisions strengthen definitions, clarify institutional responsibilities and delegated privacy functions, expand provisions relating to consent, collection, use and disclosure of health information, data breach management, research, Cultural Safety, and information security, and improve alignment with associated ACC governance, informed consent, and records management frameworks.	