Te Kaunihera Rata o Aotearoa | Medical Council of New Zealand

Privacy Policy

Policy Statement	In everything Council does, we will protect and safeguard all personal and health information we are guardians of and treat it with the utmost care, respect and discretion. In doing this we ensure that we comply with the Privacy Act 2020 and any other obligations we have relating to personal information.
Scope	The Health Practitioners Competence Assurance Act 2003 (HPCAA) gives Council authority to collect, maintain, use and share personal information and personal health information. This privacy policy covers all personal information (including health information) we collect, use, disclose and store. This includes information belonging or relating to: • Medical professionals • Patients • Employees • Agents of Council • Complainants and other members of the public.
Definitions	*Personal information* is information about an identifiable individual. Some personal information may be publically available: e.g. information on the public tab in MedSys. Note: For the purpose of this policy, 'personal information' includes 'personal health information'. *Information Privacy Principles (IPPs)* are the 12 privacy principles set out in the Privacy Act. *Official information* is any information held by the Government, including government departments, educational institutions and public hospitals. The Official Information Act is the law which controls the availability, access and protection of official information. It is important to note that, while the Medical Council is not subject to the Official Information Act, some organisations we interact with are. For example, the Health and Disability Commissioner and public hospitals. This means any information we provide them will be subject to the Official Information Act.

Standards

Collection

Council will only collect personal information if it is necessary to do so, and only for a lawful purpose connected with a function or activity of the Council. Personal information will be collected only with consent of the individual or where required or authorised by law.

The HPCAA requires collection of personal information for the purposes of applications for registration/NZREX, applications for practising certificates, competence review, conduct investigations and Health Committee assessments. We also collect information to enable us to employ and pay our employees, and manage contracts with suppliers and agents of Council.

Council collects personal information only from the individual concerned unless there is a lawful reason not to. Exceptions under the HPCAA include notifications of competence, conduct or fitness to practise; information provided by other agencies pursuant to memoranda of understanding or under authority held by those agencies; supervision reports and Health Practitioners Disciplinary Tribunal (HPDT) decisions.

When collecting personal information, the individual is to be made aware of:

- the fact that information is being collected
- why it is being collected
- who will receive the information
- whether it is mandatory or voluntary to provide the information
- the consequences of not providing the information
- their rights to access and correct the information.

Council may not collect personal information by unlawful means, or by means that are unfair or intrude unreasonably on the individual's personal affairs.

Access and Correction

Anyone may:

- obtain confirmation from the Council of whether or not we hold personal information about them; and
- have access to that information.

This information is to be made available as quickly as possible. The Privacy Officer must be consulted before any decisions are made to withhold information.

Where an individual is given access to their personal information, the individual must be informed that they may:

- request correction of their personal information;
- request that if it is not corrected, a statement is attached to the original information saying what correction was sought but not made.

Any incorrect information we hold is to be corrected as soon as we are made aware of an inaccuracy.

Use and Disclosure
We will use personal information to enable us to deliver Council's functions under the HPCAA, and to take any action we are required or authorised by law to take.

Personal information is only to be used for the purpose(s) for which it was collected, unless there is good reason to use it for other purposes and this is allowed by the Privacy Act. If there is any doubt about the purpose for which personal information was collected or is being used, the Privacy Officer is to be consulted.

Personal information about an individual is to be provided only to that individual or to other individuals or organisations they have authorised us to provide their information to, except where required or authorised by law. Where a request for an individual's information is received, your manager or the privacy officer can provide advice as to whether this information should be provided.

Before information is used or disclosed, it is to be checked to the extent possible to ensure that it is accurate, complete, up to date and relevant. Limits on disclosure of information apply to disclosure to other people and teams within the Council as well as to external organisations. Relevant personal information may be disclosed by staff internally if it is consistent with the purposes for which it was collected. A process for monitoring access to personal information and identifying inappropriate access is being implemented.

Releasing personal information to a third party is permitted provided that the procedures relating to this are accurately followed. We will provide personal information to other people or organisations if we need to do so to deliver our functions, and with consent or where required or authorised by law. We may disclose personal information, with appropriate safeguards in place, to:

- Approved employees and Agents of Council
- Medical professionals' employers
- Health care professionals, vocation education & advisory bodies, or other agencies providing information for the purposes of consideration of conduct and competence
- Our business and service providers (such as IT providers)
- Our professional advisors (such as insurers and auditors)
- Government and regulatory authorities, where required or authorised by law (including the Health & Disability Commissioner, ACC, Police, overseas equivalents of the Medical Council) and with appropriate documented agreements in place.

Examples of safeguards for disclosure of information include memoranda of understanding with external organisations, confidentiality agreements, secure means of transfer, and/or assurance over the information handling practices of external organisations. The Privacy Officer should be consulted in all new situations of personal information disclosure.

We are required to take all reasonable steps to ensure third parties protect personal information with the same care and respect we do. The memoranda of understanding in place are part of this process and must be adhered to.

Storage and Security
Council ensures information is protected by such security safeguards as it is reasonable in the circumstances to take, against loss, access modification, misuse or unauthorised disclosure.

Only approved personnel will have access to any personal information we hold. Council must do everything reasonably within its power to prevent unauthorised use or unauthorised disclosure when giving that information to a person in connection with the provision of a service to the Council.

We keep personal information only for as long as it is needed, and will destroy it securely when it is no longer needed. Personal information is not to be kept longer than needed for the purpose for which it has been collected. Council's retention and disposal schedule sets out how long information is to be kept for.

Unique Identifiers

Unique identifiers may not be assigned unless they are required to carry out our functions efficiently. Unique identifiers (registration numbers) are assigned to doctors. No other identifiers are to be used by Council.

Privacy Breaches and Incidents

A privacy breach refers to unauthorised access to or collection, use or disclosure of personal information. It is 'unauthorised' if it is not in compliance with the Privacy Act 2020 and the Health Information Privacy Code 1994.

All staff must notify their Team Leader or Team Manager **immediately** if a privacy incident is suspected or identified. The Privacy Officer must also be notified the same day of the privacy breach. The Privacy Incident Reporting Metrics process and Privacy Breach Journey are to be followed.

Once the Privacy Incident Reporting Metrics process has been completed the following actions must be taken for each level:

Level 1: Immediately inform your Team Leader and Team Manager when you become aware of the breach. You need to inform the Privacy Officer of the breach that same day.

Level 2: Immediately inform your Team Leader and Team Manager when you become aware of the breach. A meeting with the Privacy Officer, your Team Leader, and Team Manager will take place to discuss the breach and learnings. This meeting is to happen the same day if possible.

Level 3: Immediately notify the Chief Executive and the Privacy Officer.

Level 4: Immediately notify the Chief Executive and the Privacy Officer. The Chief Executive will notify the Chair of Council immediately.

Council has a 'no blame' policy and there will not be any repercussions for a privacy breach as long as the incident was accidental, reasonable care was applied, and Council policies and procedures have been followed.

However, disciplinary action may follow if:

- There is a deliberate breach of an individual's privacy. Any deliberate disclosure of personal information for purposes other than specified in this policy is considered serious misconduct.
- A privacy breach is covered up or attempted to be hidden. Not immediately notifying a Team Leader or Team Manager or Privacy Officer is considered serious misconduct.
- Avoiding or circumventing Council policies or systems which results in a privacy or security breach whether intentionally or unintentionally.
- Where a reasonable level of care is not applied when carrying out a function or your role or task assigned to you that involves personal information and a breach occurs.
- Repetitive privacy breaches.

Accountability and Responsibility

Council is responsible for ensuring that the Council has robust policies and procedures relating to personal and health information that are consistent with the relevant legislation. Council will require the CEO to give effect to this strategy.

The **Chief Executive Officer (CEO)** is responsible for building and maintaining a privacy culture that reflects the Council's values. In addition, the CEO appoints our Privacy Officer, and deals with any challenges to the decisions made by the Privacy Officer.

Our **Privacy Officer** is responsible for exercising the statutory responsibilities in the Privacy Act and providing guidance and practical advice on privacy matters to staff and Council members, including privacy incidents.

Our **ELT and team leaders** are responsible for fostering our culture of respect for personal and health information within the organisation and their teams. Managers are both individually and collectively accountable for:

- Ensuring their teams understand and comply with our privacy policies and procedures
- Actively identifying privacy risks and ensuring all privacy incidents are investigated, reported and resolved in a timely and professional manner.

Staff are expected to consistently demonstrate our culture set through their behaviour, compliance with our privacy policy and procedures, identification of privacy risks, and by reporting all privacy incidents immediately to their team leader or manager.

Council agents – our staff are expected to ensure that all Council agents are aware of Council's privacy policies and to ensure that all agents sign confidentiality or privacy agreements relevant to the role they are undertaking.

Links to other documents	• Privacy incident reporting metrics (9132654) • Policy on security of information including data on computers and security when communicating electronically (237339) • Policy on release of health information to the media (44644) • Protocol on exchange of information between Health Practitioners Disciplinary Tribunal and Medical Council of New Zealand about competence matters potentially indicating a risk to members of the public (44679) • Protocols for communication with complainants and other stakeholders (3112442 • Protocol for receipt and actioning of privacy requests pursuant to the Privacy Act 2020 and the Health Information Privacy Code 1994 (22275) • Confidentiality agreement • Policy – Email • Procedures for information of the Medical Council of New Zealand • Protocol – Record Keeping • Protocol on what information may be disclosed about health clients involved in other Council processes • Incident Management Process • Procedure for identifying and sharing personal information
Approvals	Document owner: Deputy Registrar Reviewed by the Management Committee: 15 April 2019 Current version approved by the Chief Executive: 15 April 2019 Next review date: April 2021 The Chief Executive reserves the right to review this policy at any time in consultation with Management, and subject to the approval process.