Policy on management of personal information

Policy Statement	The Health Practitioners Competence Assurance Act 2003 gives Council authority to collect, maintain, use and share personal information and personal health information. The purpose of this policy is to provide direction for staff on how to give effect to the HPCAA and exercise the authority given to Council in a way that is consistent with the requirements of the New Zealand Privacy Act 1993 (the Privacy Act) and the Health Information Privacy Code 1994 (the Code).
Scope	This policy applies to all Council members, Council employees and agents (including PAC, VPA and PCC members) and contractors that we engage.

Definitions

Personal information is information about an identifiable individual. It must be treated with respect at all times and in accordance with the Privacy Act 1993.

Some personal information may be publically available: e.g. information on the public tab in MedSys.

Personal health information is information about an identifiable individual's health.

The Code applies specific rules to health agencies. Most health information is collected in a situation of confidence and trust, is often highly sensitive, and may be required long after it has ceased to be to be needed for the original care or treatment. When health information is collected, used, held or disclosed the rules in the Code must be applied unless the HPCAA overrides these.

Note: For the purpose of this policy, 'personal information' includes 'personal health information'.

Privacy incident is unauthorised access to or collection, use, or disclosure of personal information. Such activity is 'unauthorised' if it is not in compliance with the Privacy Act 1993 and the Code.

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.

Important note
While the Medical Council is **not** subject to the Official Information Act, some organisations we interact with are. For example, Health and Disability Commissioner and public hospitals. This means any information we provide them will be subject to the Official Information Act.

Privacy Officer	Section 23 of the Privacy Act states that all agencies must have at least one Privacy Officer. The Council's Privacy Officer is appointed by the Chief Executive. The role of the Privacy Officer is to advise the business and handle privacy related matters. For any queries in relation to this policy and privacy in general, consult the Privacy Officer.

This section sets out

- summarised IPPs
- relevant HPCAA-based statutory powers, and
- related Council policy/practice

Information privacy principles (in summary)	**Applicable HPCAA powers and policy**	**Council meets these requirements by:**
Purpose for which information may be gathered – Principle 1		
The Council may only collect personal information if it is necessary, and for a lawful purpose connected with a function or activity of the Council.	Applications for registration/NZREX Applications for practising certificates Competence review Conduct investigations Health Committee assessments	Prescribing the information that must be provided as part of an application.
Source of personal information – Principle 2		
The Council must collect this information from the individual concerned except in certain situations	Notifications of competence, conduct or fitness to practise under the HPCAA, HDCA or ACA. Information provided by other agencies pursuant to MOUs or under authority held by those agencies Supervision reports HPDT decisions	Collecting personal information directly from the individual concerned or someone authorised by the individual or by the individual's authorised agent. Documenting in the individual's file when information is not collected directly from the individual: • the source of the information • the identity of the person providing the information • any compliance obligation with other legislation is required (e.g. the Mental Health Act, Crimes Act, etc). Information from other sources

		will be made available to the individual concerned
Requirement to inform individual about collection, sharing and use of information – Principle 3		
When collecting personal information, the individual must 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.	These include many aspects of our statutory functions, through registration, practising certificates, performance, health, conduct, the register, and policies, Council's protocols for communication with complainants and other stakeholders	Making clear statements on Council application forms Letters to doctors requesting information (eg professional standards and health letters) will provide this information Some relevant information is covered on our Website
Manner of collection must be lawful and fair and appropriate – Principle 4		
The Council may not collect personal information by unlawful means, or by means that are unfair or intrude unreasonably on the individual's personal affairs		
Storage and security of personal information – Principle 5		
Council must ensure information is protected by such security safeguards as it is reasonable in the circumstances to take, against loss, access modification, misuse or unauthorised disclosure 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	*Refer to the **policy for staff on security of information** for further guidance.*	The Council will ensure that there are reasonable safeguards against loss, misuse, unauthorised access or disclosure of personal information. These safeguards include: • physical (location of records and computers) • operational (employee confidentiality agreements, information management policies, auditing access to information) • technical (use of passwords, tracking access to information, EDRMS systems).

Individual entitled to access to personal information – Principle 6		
An individual is entitled to - • obtain confirmation from the Council of whether or not it holds personal information; and • have access to that information. Where an individual is given access to personal information, the individual must be informed that they may request the correction of that information.	The Privacy Act sets out limited grounds to refuse to give individuals access to their personal information	The Privacy Officer should be consulted before any decisions are made to withhold information.
Correction of personal information – Principle 7		
Where the Council holds personal information, the individual concerned is entitled to: • 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.	*For further guidance refer to **correction of personal information** procedure document.*	Personal information can be corrected if the request is factual and evidence can be provided to support the request Before decision making occurs, assessment reports are provided to doctors for comment and correction of factual errors. If a conclusion is contested, this is referenced to the relevant document
Accuracy, retention and limits on both use and disclosure of personal information – Principles 8 – 11		
Accuracy (Principle 8) Before information is used or disclosed, it should be checked that it is accurate, complete, up to date and relevant. **Retention (Principle 9)** Personal information is not kept longer than needed for the purpose for which it has been collected it.	The Clean Slate Act may be relevant Information on registration, performance, health, conduct and the register is retained throughout a doctor's practising life.	If detailed notes are made of information taken by phone that cannot be easily read back, and it may be used in decision making, the notes should be provided to the caller to confirm accuracy. Personal information is not kept longer than needed for the purpose for which the Council or its agents collected it. These requirements are also in the

Limits on use (Principle 10) Personal information will only be used for the purpose that it was collected. If there is any doubt about the purpose for which personal information is being used for, consult the Privacy Officer.		Council's information management policies.
Disclosure (Principle 11) see IPP 11 for what is considered reasonable	Other circumstances where personal information can be disclosed are detailed in Appendix 4 – Procedure for identifying and sharing personal information	Relevant personal information may be disclosed by staff internally if it is consistent with the purposes for which it was collected. Releasing private information to a third party is permitted provided that the procedures relating to this are accurately followed. For example, third party requests may be received from: • ACC • HDC • DHBs • PHOs If there is any doubt about a third party request for personal information, the Privacy Officer must be consulted. There are also situations where we proactively share personal information with third parties. For further guidance refer to Appendix 4.
Use of unique identifiers – Principle 12		
May not be assigned unless they are required to carry out our functions efficiently		Unique identifiers (reg numbers) are assigned to doctors in MedSys

Non-compliance / breaches	The Council values trustworthiness, openness and accountability, and integrity. To uphold these values staff are expected to report immediately any privacy incident to their Team Leader/Manager.

Links to other documents	• Policy for staff on security of information (including data on computers) (237339) • Policy for Council members and agents on security of information stored on computers or carried from place to place (44537) • 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 • Memoranda of understanding outlining communication with third parties involved in our processes around addressing concerns about a doctor's practice • Protocol for receipt and actioning of privacy requests pursuant to the Privacy Act 1993 and the Health Information Privacy Code 1994 (22189) • Confidentiality agreement • Procedure for distinguishing, sharing and correction of personal information • Stakeholder communications strategy
Approvals	Document owner: Philip Pigou Reviewed by the Management Committee: Current version approved by the Chief Executive: 4 December 2017 Next review date: The Chief Executive reserves the right to review this policy at any time in consultation with Management, and subject to the approval process.

Appendix 1

Privacy Risk Assessment Template

Risk management objectives	• Develop a 'risk aware' culture that encourages Council and its agents to identify risks and associated opportunities in a planned and coordinated manner, and to respond to them with cost effective actions. • Be risk prepared through high levels of risk awareness, risk management competence, and appropriate tools and resources. • Achieve tangible and sustainable performance improvement. • Enable achievement of long-term business objectives. • Be seen as an organisation that manages its risks responsibly. Council's general risk appetite will be conservative and its tolerance will be risk-averse.

Definitions

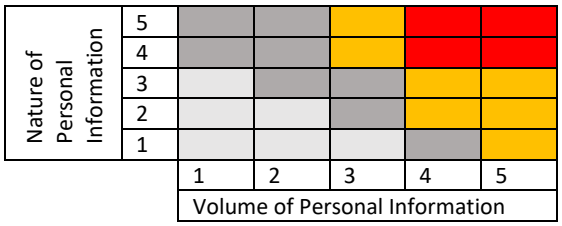
For the purpose of this policy, unless otherwise stated, the following definitions will apply:

- **Risk** is the effect of uncertainty on achieving objectives. Risk is the correlation between likelihood and consequences of an event occurrence.
- **Privacy risk** is the risk that the Council breaches an individual's rights in relation to privacy, or loss, damage, misuse or abuse of their personal information. It also includes the risk the Council operations do no align with our privacy values as set out in the Privacy Strategy.
- **Risk assessment** is the process of risk identification, risk analysis and risk evaluation.
- **Risk management** are the coordinated activities that direct and control Council with regard to risk.
- **Personal information is any identifiable information about an individual.**

Privacy risk assessment – process/system

This privacy risk assessment is to identify the privacy risks and the strength of the controls within Council processes and systems. The privacy risk assessment should be conducted as a workshop with relevant stakeholders. The outcome of the assessment is to identify control weaknesses and/or gaps, so that appropriate remedial action can be taken.

Question	Answer
Process/system	
Is personal information collected, used or disclosed in this process/system?	(Y/N – if 'Yes', please state whether personal information is collected, used and/or disclosed)
Do you know where personal information is held (personal information locations and files)?	(Y/N – if Yes, please list)

What format(s) is the personal information stored in (paper, electronic, CD, USB, cloud etc.)?	(Please list)
What are the key types of personal information collected, used, disclosed?	(Please list)
Nature of information 1 = Non-identifying 2 = ↕ 3 = Individual personal information 4 = ↕ 5 = Sensitive information about individuals	
Volume of information 1 = Ad-hoc; one-off information 2 = ↕ 3 = Moderate volumes 4 = ↕ 5 = Large volumes	
Inherent risk – that is the privacy risk with no controls in place.  Risk Level: Significance Level 1: Low Level 2: Moderate Level 3: High Level 4: Critical	
Key controls:	
Segregation of duties	
Restricted access	
Change management	
Other (please list)	
Other (please list)	
Other (please list)	
Other (please list)	
Overall control strength H = High M = Medium L= Low	

Residual risk – that is the privacy risk with the controls in place.

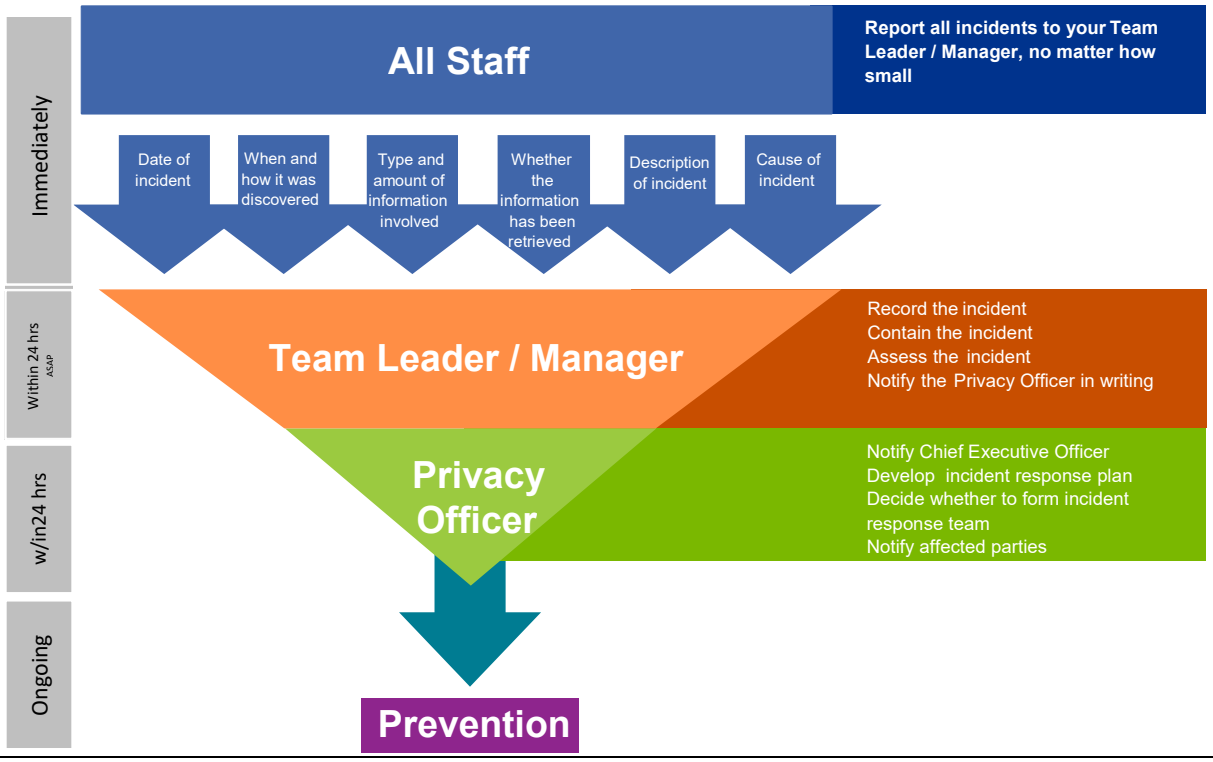
Risk level	Significance
Level 1	Low
Level 2	Moderate
Level 3	High
Level 4	Critical

Appendix 2

Incident management process

The Council has a policy of openness and accountability when dealing with privacy incidents. All staff are expected to report all incidents immediately.

Overview of Process



Detailed Process

Outlined below is the detailed incident management process for dealing with a privacy incident.

Step	Action	Responsibility	Timeframe
1	**Report to Team Leader/Manager** a. Even if an incident is only suspected it is important to report it to your Team Leader/Manager as soon as you become aware of the situation. b. Provide as much information as possible – this will mean corrective action can be taken more quickly and effectively. Valid information to be provided includes: i. Date of the incident ii. When and how the incident was discovered iii. Whether information has been retrieved, for example by: • successfully recalling an email • telephoning an unintended email recipient and asking them not to read an email and to delete it from their email (both inbox and deleted folder) • liaising with the courier about redirection • telephoning an unintended postal recipient to arrange for the return of the item unopened iv. Cause of the incident v. Type and amount of information involved. c. This information must be recorded in the incident log by the Team Leader.	Staff who are responsible for, or discovered the incident	Immediately
2	**Contain the incident** The aim of this step is to prevent any further incidents from occurring in the same manner. Possible measures include: a. Recover the information b. Isolate/suspend the process or system c. Revoke computer/physical access rights d. Any actions taken must be recorded by the Manager in the incident log.	Team Leader / Manager	a. Immediately b – d. As soon as practical

3	**Investigate and assess the situation** Consider the impact/risk of the incident. Any high risk incidents should be immediately reported to the Privacy Officer and the Chief Executive. Consider the following: a. What personal information was involved in the incident? b. How potentially significant is the information? The more sensitive or high profile the information, the higher the risk associated with the information. Apply the 'front page of the Dominion' test. c. Is the personal information protected / anonymised in some way that means that it is not easily accessible? Information that is not easily accessible and can be quickly recovered has a lower risk associated with it. d. Who received the information? If there any relationship between the recipient and the person whose privacy was breached? e. Consider the type and amount of personal information involved and how it could potentially be used. f. Is there a reasonable possibility that the Privacy Commissioner, the Minister of Health, or the media will be notified of the incident?	Manager	Immediately
	Incident response plan – depending on the risk assessment Where appropriate form an Incident Response Team to deal with the repercussions of the incident. a. Form an Incident Response Team made up of relevant stakeholders including: i. Privacy Officer. ii. Chief Executive. iii. Communications Manager. iv. Management team. v. Other subject matter experts and key stakeholders. b. Develop Incident Response Plan i. Prioritise actions. ii. Identify roles, responsibilities, and timeframes. iii. Consider impact on business as usual.	Privacy Officer / Chief Executive	Within 24 hours

4	**Notify affected parties** While the Privacy Act does not require agencies to notify individuals of a privacy incident, the Council has a policy of openness and transparency. a. The notified individual should be given a verbal apology and a description of the personal information involved, the general timing of the incident and an overview of the corrective action which has been taken. b. A written apology should be sent to confirm the information given verbally c. The CEO will decide whether information needs to be sent to the Privacy Commissioner, the Minister of Health about the incident.	Privacy Officer	Within 24 hours
5	**Prevention** a. Identify the root cause of the incident and assess whether there is a risk of ongoing incidents. b. Was this a one-off incident, or is it the result of a systemic issue? c. What steps have been taken to mitigate the incident? Are these steps short-term preventative measures or aimed at addressing the issue for the long term? d. For recurring or systemic issues a prevention plan should be developed and may include the following: i. Review of privacy policies and procedures ii. Review of training and education provided to staff iii. Adjustments to technical and physical security iv. Assessment of effectiveness of incident management v. Implementation plan for corrective action, including responsible person and timeframes.	Manager / Privacy Officer depending on whether incident was escalated	Ongoing

MCNZ Privacy incident reporting template

Appendix 3

Date of incident	Date of discovery	Team	Person(s) whose privacy was breached	Description of incident	How was it discovered	Relevant IPP breached (1-12)*	Action taken	Status of incident (open/resolved)

Information privacy principles (IPP)

1. Purpose of collection of personal information
2. Source of personal information
3. Collection of information
4. Manner of collection of personal information
5. Storage and security of personal information
6. Access to personal information
7. Correction of personal information
8. Accuracy of personal information to be checked before use
9. Personal information not to be kept for longer than necessary
10. Limits on use of personal information
11. Limits on disclosure of personal information
12. Unique identifiers

Procedure for identifying and sharing personal information

This document:

- explains how to identify personal information and explains the Council's obligations in this regard
- establishes procedures to enable staff to share personal information responsibly and in line with the privacy policy, Privacy Act and Health Information Privacy Code (the Code).

  Note: refer to the Code if dealing with health information

Requests for Information	Under the Privacy Act, individuals have the right to access personal information.
Sharing personal information	Information Privacy Principles 8 – 11 of the Privacy Act restrict how personal information can be used or disclosed. Personal information will only be used for the purpose that it was collected. There are instances where personal information can be used for purposes other than what it was collected for such as protecting public health or safety. If there is any doubt about the purpose for which personal information is being used for, consult the Privacy Officer. Before staff use or disclose personal information, it should be checked that it is accurate, complete, up to date and relevant. Personal information is not kept longer than needed for the purpose for which the Council collected it. These requirements are also in the Council's information management policies. When sharing personal information consider the following: • Is there a clear and legitimate purpose for sharing the information? • What information may be shared? • Is it health information which needs to be treated as highly sensitive? • Do you have consent to share the information? • Have you verified the source requesting the information? • How will you share the information appropriately securely? • Who can the party requesting the information share the information with? • Could it be subject to an OIA if provided to the requestor? • Would the Clean Slate Act be applicable to any information we might hold?
Sharing personal information internally	Relevant personal information will be used and disclosed by staff within the Council as much as is required for efficient and effective case management purposes.
Sharing personal information externally	Personal information may be shared externally if authority from the individual concerned has been given and it is consistent with the purposes for which it was collected OR when information is shared with third parties in accordance with our MoUs and communications protocols under the authority of section 157 of

	the HPCAA. The procedures outlined in this document must be followed when sharing personal information. Requests to share personal information may come from the following: • a lawyer • Accident Compensation Corporation • Health & Disability Commissioner • Orders for publication • insurers • Police.
Procedures	1. All requests for information must be considered by the Deputy Registrar in the first instance. 2. After assessing whether personal information can be shared, staff must ensure the method for sharing that information is appropriate, secure and protects the integrity of the information while in transit. 3. Before any personal information is disclosed staff must take reasonable steps to ensure that the information is accurate, complete, up to date and relevant. 4. A filenote must be created to document when personal information is shared and who with unless it is obvious from covering correspondence.
Methods of sharing personal information	**Email** 1) Check the email address is correct. 2) Avoid sending email attachments if it can be helped. 3) Convert to a pdf wherever possible. 4) Where appropriate, encryption or password protection should be used. 5) Double check the content and attachment of the email before sending. 6) Save relevant emails to the DM. 7) Ensure your email signature includes an "unintended recipient" disclaimer. **USB/CD** 1) Encrypt the USB with a password. 2) Password protect documents on the USB. **Courier or post** 1) Check the postal address is correct. 2) Ensure the envelope/package is secure. 3) Ensure the Medical Council return contact details are on the outside of the envelope/package. 4) Ensure track and trace is used requiring the recipient to sign on receipt. **Basecamp** Where appropriate, Basecamp is to be used for sharing information with external agents/stakeholders, including Council and Committee agendas.

Physically

Staff taking personal information off the premises as a physical document must ensure it is stored securely. For example in a 'non-transparent' folder or in a locked bag. *Refer to policy for Council members and agents on security of information stored on computers or carried from place to place.*

Procedure for correcting personal information

This document explains the procedures for staff to respond to requests to correct personal information in line with the privacy policy, Privacy Act and Health Information Privacy Code.

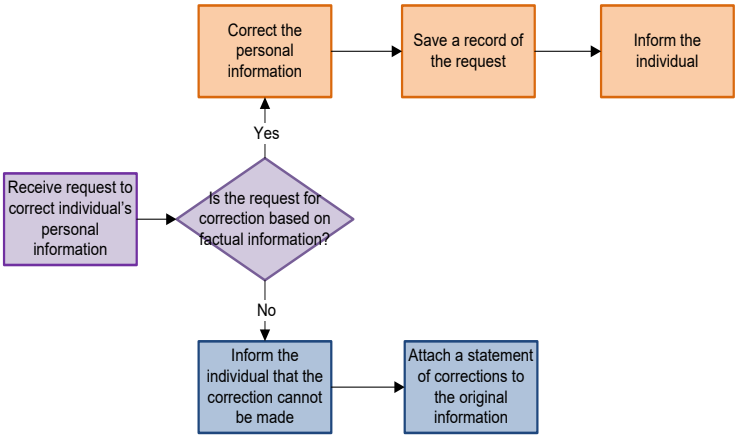
Correction of personal information

Information Privacy Principle 7 states that everyone is entitled to:

- 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.

Procedures for correcting personal information

The diagram and guidance below sets out the process for assessing when personal information can be corrected and how to process the request.



These steps set out the process that staff who receive requests for correction of personal information must follow:

1) Request the individual provide the request in writing with appropriate supporting evidence.

2) Determine whether the request is appropriate and correction can be made.

   Personal information can be corrected if the request is factual and evidence can be provided to support the request. If evidence cannot be provided but the Council agrees the request is factual and appropriate the information can be corrected.

   A correction to personal information cannot be made if the request is subjective and not factual. An example would be an opinion formed by an assessor, which could be contested but not considered factually incorrect.

Examples of personal information that can be corrected include:

- contact details such as phone numbers or physical and email addresses
- name, for example change of surname, or misspelt names
- factual errors in reports, documents, databases, registers, certificates and so on.

Staff may consult the following staff when considering the request for correction if they are unsure:

- Privacy Officer.
- Team Leader or Manager.

3) Process the request as outlined below ensuring to respond to the individual who sent the request within 20 days of receiving it.

If the correction can be made

- correct the requested piece of information
- save a record of the request
- inform the individual the correction has been made.

If the correction cannot be made

- inform the individual in writing that the change cannot be made to the original record but that a statement of correction outlining the requestor's position will be attached to the original file document
- advise the individual of their right to make a complaint to the Privacy Commissioner
- attach a statement to the original information (usually in DM) saying what correction was sought but not made.

Example – *A Doctor requests a correction to a reference about them by someone else which is subjective. The request is subjective and therefore the correction cannot be made. Inform the Doctor in writing. Scan the original request and save it in MedSys under the doctor's registration number and 'relate' it to the relevant document.*