Canterbury
District Health Board
Te Poari Hauora ō Waitaha

CORPORATE OFFICE

Level 1
32 Oxford Terrace
Christchurch Central
CHRISTCHURCH 8011

Telephone: 0064 3 364 4134
Kathleen.Smitheram@cdhb.health.nz;

23 May 2022

9(2)(a)
[redacted]

RE Official Information Act request CDHB 10837a

I refer to your letter dated 12 April 2022 and received in our office on 29 April 2022 requesting the following information under the Official Information Act from Canterbury DHB. This is a followup request to our earlier response CDHB 10837. Specifically:

1. **Copies of the "helpful links" that are referenced within the Code of Conduct:**
   - **a) Active bystander online module (in the minimum, screenshots)**
   - **b) Maintaining A Bullying, Harassment and Discrimination Free Workplace Policy**
   - **c) Conflict of Interest and Disclosure Policy**
   - **d) Information Security Management Policy**
     This policy has been reviewed and pending approval will be replaced with two documents – Information Management Policy and ICT Security Responsibilities Policy.
   - **e) Privacy Policy**
     A new policy, reflecting the Privacy Act 2020 and Health Information Privacy Code 2020, has been completed and is going through the process of implementation.
   - **f) Health Privacy module (in the minimum, screenshots)**
   - **g) Disciplinary Policy**

Attached in **Appendix 1** are policies from CDHB Code of Conduct, provided in our earlier response CDHB 10837.

Included are screenshots for 1a) and 1f). These screenshots are for HELM and healthlearn, websites and learner management systems with access only for CDHB and WCDHB staff. HELM is the CDHB and WCDHB inhouse website for leadership learning and development. It's our portal for learning resources, workshops and courses plus our foundational Leadership Koru. healthLearn is our Learner Management System i.e., our digital platform up which sits all our on-line courses. It's the place where people enrol into courses, have their learning attendance recorded, and complete course participation.

2. **Copies of information you hold on professional registration bodies, professional standards and ethics for:**
   - **nurses**
   - **psychologists**
   - **social workers**
   - **occupational therapists**
   - **psychiatrists**
   - **neurologists**

Professional registration bodies host their own registration, standards and ethics. As the CDHB does not hold this information, we are therefore declining pursuant to section 18(g) of the Official Information Act i.e. we do not hold this information.

We provide links to websites pertaining to your request.

- **nurses**

Nursing Council of New Zealand
https://www.nursingcouncil.org.nz
https://www.nursingcouncil.org.nz/Public/Nursing/NCNZ/Nursing.aspx?hkey=4c7f36f6-42c3-40fa-b35c-88875eb2dcd5

- **psychologists**

New Zealand Psychologists Board
https://psychologistsboard.org.nz/
https://psychologistsboard.org.nz/for-practitioners/the-code-of-ethics-for-psychologists-working-in-aotearoa-new-zealand/

- **social workers**

Social Workers Registration New Zealand
https://swrb.govt.nz/
https://swrb.govt.nz/about-us/policies/

- **occupational therapists**

Occupational Therapy Board of New Zealand
https://www.otboard.org.nz/
https://www.otboard.org.nz/site/ces/codeofethics?nav=sidebar

- **psychiatrists**
- **neurologists**

For doctors (including psychiatrists and neurologists) all standards are laid down by the Medical Council of New Zealand (MCNZ).
https://www.mcnz.org.nz/

I trust that this satisfies your interest in this matter.

Please note that this response, or an edited version of this response, may be published on the Canterbury DHB website after your receipt of this response.

Yours sincerely

Ralph La Salle
Senior Manager, OIAs
Canterbury DHB & West Coast DHB

Appendix 1

Appendix 1a - Active bystander online module (in the minimum, screenshots)

HELM is the CDHB and WCDHB inhouse website for leadership learning and development. It's our portal for learning resources, workshops and courses plus our foundational Leadership Koru.

Maintaining a Bullying, Harassment and Discrimination Free Workplace Policy

Purpose

This policy sets out the Canterbury District Health Board and West Coast District Health Board (referred to as **our** or **we**) approach and commitment to maintaining a bullying, harassment and discrimination free workplace; and provides the foundation for us to meet our obligations under the Health and Safety at Work Act 2015.

Policy

We are committed to providing a safe workplace for all our people. We recognise that maintaining a workplace free of bullying, harassment and discrimination ensures:

- our people enjoy being in the workplace and remain in the workplace due to a positive work culture; and
- the safety of our people, patients or visitors is not compromised.

All our people have the right to work in an environment free from bullying, harassment and discrimination. We will therefore not tolerate bullying, harassment and/or discrimination in the workplace and we encourage our people to speak up where they are subject to or witness bullying, harassment and/or discrimination in the workplace

1. Bullying, Harassment and Discrimination

Note: These terms are not mutually exclusive, so harassment and/or discrimination can be part of bullying.

1.1. Bullying

Bullying is *unreasonable and repeated behaviour* towards a person or group that can lead to physical or psychological harm.

Repeated behaviour is persistent and can include a range of actions. Unreasonable behaviour covers actions which a reasonable person wouldn't do in similar circumstances, including, but not limited to, victimising, humiliating, intimidating, threatening or excluding a person or group.

A single incident isn't considered bullying but can escalate if ignored. Managing performance in line with policies and processes is not bullying.

1.2. Harassment

Harassment is behaviour, direct or indirect, whether verbal, physical or otherwise towards a person or group that:

- Is unwanted and unjustified;
- Is offensive or humiliating to the person or group; and
- Is so serious and/or repeated that it may have a detrimental effect on the person or group's job performance and/or job satisfaction.

This is most commonly sexual or racial harassment but can include other forms.

1.3. Discrimination

Discrimination is behaviour where a person is disadvantaged on the grounds of age, race or colour, disability, sexual orientation, sex (incl. pregnancy or childbirth), religion, spiritual or ethical belief, marital or family status, political opinions, employment status, gender identity or expression, ethnicity or national origins, being affected by domestic violence or being involved in union activities.

2. Managing Complaints

We have processes in place for making and managing complaints to ensure any complaint or query is treated confidentially, taken seriously and acted on promptly. The options, reporting and process steps are detailed on max.

In summary, we must:

- Support all parties involved;
- Find appropriate remedies and consequences for confirmed bullying, harassment and/or discrimination, as well as false reports; and
- Ensure confidentiality.

3. Disciplinary Action

Bullying, harassment and/or discrimination may amount to misconduct or serious misconduct and could result in disciplinary action up to and including dismissal. Our Disciplinary Policy provides details about this process and the potential outcomes.

Applicability

This policy applies to all our employees, contracted individuals, volunteers, visiting health professionals and students (referred to as **our people**).

This policy applies where bullying, harassment and/or discrimination is directed at our people, as well as toward a patient or visitor.

Roles and Responsibilities

Our people should:

- Speak up if they experience or see any bullying, harassment and/or discriminatory behaviours and;
- Accept that misunderstandings between our people can occur which can lead to an unjustified perception that bullying, harassment and/or discrimination is taking place.

We should:

- Recognise that preventing and addressing bullying, harassment and/or discrimination in the workplace is essential to meeting our obligations under the Health and Safety at Work Act 2015.
- Provide our people who feel they've been bullied, harassed and/or discriminated against with a range of options to resolve the issue.
- Promote informal or direct solutions before formal actions where appropriate. Our people can seek guidance on this on max and/or speak to People and Capability for assistance.
- Aim to repair the working relationship and promote positive work values.

Policy measurement

We will measure the number of formal complaints received regarding bullying, harassment and discrimination. This will be reported annually. All data will be reported anonymously to preserve the privacy of our people.

Associated material

- Doing the Right Thing – Our Code of Conduct
- Disciplinary Policy
- Diversity and Inclusion Policy

References

- Employment Relations Act 2000
- Human Rights Act 1993
- Health and Safety at Work Act 2015.
- WorkSafe NZ Good Practice Guidelines - Preventing and responding to bullying at work 2017.

Contents

Conflict of Interest and Disclosure of Interest Policy

Contents

Purpose

Canterbury DHB and West Coast DHB (referred to as **DHB, we** or **our**) are committed to providing a fair, ethical and accountable environment. Our primary concern for is for the safety and welfare of our patients, our people and the communities in which they live. This central principle of healthcare can, however, be compromised by Financial and Non-financial Interests that lead to Conflicts of Interest.

This policy provides guidance on:

- what constitutes a Conflict of Interest;
- recognising and disclosing Conflicts of Interest; and
- the process for notifying and managing Conflicts of Interest.

Policy

Our people must conduct themselves with integrity, honesty and diligence in performing their duties for the DHB and avoid placing themselves in situations where their private Interests are, may be, or are perceived to conflict with the interests of the DHB.

Sometimes a Conflict of Interest is unavoidable, however we need to put practices in place to ensure that all conflicts are disclosed and managed, so we can protect the interests of our patients, our people and the business.

Our people have an on-going obligation to disclose and manage any Financial or Non-financial actual, perceived or potential Conflict of Interest, including any

alternative employment, in a timely and effective manner via the max. disclosure process.

The Executive Management Team and all General Managers are required to disclose all non-DHB roles or Interests that they (or a Related Party) have regardless of whether it may conflict with their DHB role and responsibilities.

Scope

This policy applies to:

- all DHB employees, including, temporary employees, contractors, independent consultants and visiting health professionals contracted to the DHB; and
- any person who is involved in the operation of the DHB, joint appointments with third parties, students, volunteers and those persons with honorary or unpaid employee status.

The reference to **our people** in this policy means all the above.

Definitions / Interpretation

Conflict of Interest means:

- a Transaction in which an individual's private (or a Related Party's) Interests may affect their judgement in acting in the best interest of, and carrying out their responsibilities for, the DHB;
- where an individual (or a Related Party) uses their DHB role, confidential information, time, material or facilities for private gain or advancement or the expectation of private gain or advancement;
- when an individual (or a Related Party), is directly or indirectly affected by the outcome of a decision to be made or a Transaction entered by the DHB.

Conflicts can be actual, perceived or potential:

- *Actual conflict is* where the conflict already exists. A direct conflict between an individual's DHB duties and responsibilities and their private Interests.
- *Perceived conflict* exists where it could be, or appears to be, that an individual's private Interests could improperly influence the performance of their DHB duties and responsibilities.
- *Potential conflict* arises where an individual has private Interests that could in the future conflict with their DHB duties and responsibilities.

Financial Interest is an interest that has monetary or other material gain. Examples include:

- shareholding or board memberships;

- paid employment, including consultancies, commissioned fee-paid work, speaker fees, fees provided in return for an expert opinion and performance bonuses tied to outcomes;
- fellowships, research, continuing education and education grants; or
- travel grants, conference expenses, donations, sponsorships, gifts and hospitality (refer to Gift, Donations, Sponsorships and Corporate Hospitality Policy).

Interest means something that brings advantage to, or affects, someone or something and can be Financial or Non-financial.

Non-financial Interest is an Interest that does not have a monetary component. It may arise from a personal relationship, or involvement with a non-profit organisation, or conduct, or beliefs that indicate prejudice or predetermination. It can include goals, enhancements of career and the possibility of acquiring professional recognition, status or fame.

Related Party means family members or other close business or personal relationships.

Transaction means:

- the exercise or performance of a function, duty or power;
- an arrangement, agreement or contract (may be Financial or Non-financial); or
- a proposal to enter into an arrangement, agreement or contract (may be Financial or Non- financial).

Managing and Monitoring

Managers

Managers will receive an electronic notification via max of all disclosures made by their team.

A Manager must:

1. review all disclosures;
2. ensure that the action proposed to manage each disclosure is appropriate and where necessary make any further comments; and
3. confirm their acknowledgement of the disclosures.

Executive Management Team and General Managers

At regular intervals, each EMT member and General Manager will receive an electronic report of all the disclosures made by their team. They must review each disclosure to ensure that the appropriate management and monitoring of any potential, perceived or actual conflict is in place and that all disclosures have been acknowledged by the relevant Manager.

People and Capability

A central disclosures register will be automatically populated and will keep a record of all disclosures that are made. People and Capability will monitor the register to ensure continued operation of the process and oversee the provision of annual reports to General Managers, EMT and the Quality, Finance, Audit and Risk Committee where appropriate to ensure appropriate management and monitoring actions are still in place.

Measurement or Evaluation

This policy will be measured by evidence supporting compliance with the policy and procedures, including any reports to management and the Quality, Finance, Audit and Risk Committee where appropriate.

Sanctions for Non-compliance

Where our people fail to comply with this policy, including but not limited to, knowingly fail to disclose and/or manage a Conflict of Interest, or have acted to their own advantage, such non-compliance will be dealt with under the Disciplinary Policy and Code of Conduct.

Privacy

It is acknowledged that disclosing Conflicts of Interest and other Interests under this policy may involve disclosing personal information. This information will be handled according to our Privacy Act obligations.

Associated Documents

Informed Consent Policy

Sensitive Expenditure Policy

Ethics of Association Policy

Fraud Policy

Code of Conduct

Disciplinary Policy

Privacy Policy

Gift, Sponsorship, Donations and Corporate Hospitality Policy

Guidance Note #1- Disclosure, Managing and Monitoring

Guidance Note #2 – Conflict of Interest Examples and Guidance

References

http://www.ssc.govt.nz/integrityandconduct

http://www.oag.govt.nz/2007/conflicts-public-entities

http://www.ssc.govt.nz/code

http://www.ssc.govt.nz/code-guidance-stateservants

http://www.ssc.govt.nz/code-resources-organisations

http://www.business.govt.nz/procurement/for-agencies/key-guidance-for-agencies/the-new-government-rules-of-sourcing

Policy Owner	Chief People Officer
Policy Authoriser	Executive Management Team
Date of Authorisation	November 2019

Information Security Management Policies

Contents

Introduction

The Board and Executive Management team of Canterbury District Health Board (Canterbury DHB) are committed to an Information Management programme that assures the security, confidentiality, availability and integrity of patient, staff and organisational

information, information processing systems and information processing resources.

Purpose

This document defines the management processes and specific information security controls that are employed to ensure that Canterbury DHB information, and computer information systems and resources, are adequately safeguarded and protected and that threats, vulnerabilities and risks are recognised, understood and minimised.

Policy

It is Canterbury DHB policy that all information used in the course of business is considered an asset and as such, managers and staff are responsible and accountable for its protection.

Objectives

The objectives of the Canterbury DHB Information Security Policy are to:

- Protect Canterbury DHB information assets, patient records and other confidential and sensitive information, from accidental or intentional disclosure, damage, modification, denial of use, or total or partial loss.
- Safeguard Information Technology (IT) resources and equipment from unauthorised access and use.
- Acquaint Canterbury DHB management and staff with information security risks and provide guidelines to assist in minimising or eliminating these risks.
- Clarify responsibilities and duties, and highlight individual employee accountability, in respect to the protection of Canterbury DHB information assets, patient records and other confidential and sensitive information.
- Establish a basis for the assessment and audit of security controls.

Scope

Persons

The policies in this document apply to all persons who access and use Canterbury DHB electronic information on Canterbury DHB information systems. Such persons include but are not limited to:

- Permanent Canterbury DHB staff
- Temporary staff and contractors.
- Visiting medical specialists, practitioners and consultants.
- Students, eg. Medical, Psychology, Nursing, Allied Health, etc.
- Vendor, supplier or other third party employees.

Electronic Information

This document covers information which is processed by, recorded by, stored in, shared with, transmitted to, or retrieved from an electronic device such as a computer, information system or handheld or mobile device (laptop, personal digital assistant, smartphone).

The terms information, electronic information and data are used interchangeably.

Information Systems

The policies apply to all computer and electronic information processing systems owned or administered by Canterbury DHB. Only information handled via computers or computer networks is covered. Although the policies include mention of other information mediums, such as voice or paper, they do not directly address the security of information in these forms.

Responsibilities

Overall Responsibility

Information security is the responsibility of the Canterbury DHB Board, Executive Management Team, management and staff.

Users

Users of Canterbury DHB computer systems and electronic information are responsible for familiarising themselves with and complying with all Canterbury DHB policies, practices and procedures dealing with information security. This includes but is not limited to:

- Using all appropriate measures and safeguards to protect information and equipment.
- Ensuring personal user identifiers, passwords, and digital certificate keys are kept confidential and not shared.
- Reporting information security incidents and breaches.
- Not purposely attempting to subvert or bypass security measures.

Partners and Third Parties

In order to gain access to Canterbury DHB information or information systems, all business and healthcare partners, third party organisations and their respective staff have a responsibility to comply with Canterbury DHB security policies.

This responsibility should be embedded in contracts or agreements between parties.

Outsourcing

The security of Canterbury DHB information must be maintained when the responsibility for information systems processing has been outsourced to another organisation.

A formal contract must be in place that addresses the security responsibilities detailed in this document.

Service Level Management

A service level management process should be available in order to maintain and improve the confidentiality, availability and integrity of Canterbury DHB information systems.

Information Sensitivity

There are two types of confidential and sensitive information recognised in Canterbury DHB information systems:

- Health information collected and controlled in accordance with the Health Information Privacy Code 1994 or with other relevant health-related legislation.

- Information that is confidential and sensitive for other reasons; such information might include financial or contractual information, human resources information, or other information that the organisation considers sensitive.

Accordingly all information contained in Canterbury DHB information systems must be protected at all times.

Ownership of Information

All personal information about identifiable individuals is owned by the individual concerned. Such information is in Canterbury DHB's care and custody and Canterbury DHB has a statutory responsibility under the Privacy Act 1993 and the Health Information Privacy Code 1994, for its storage and security.

All other information stored on Canterbury DHB computer systems and IT equipment is the property of Canterbury DHB, and the organisation reserves the right to examine that information. It is not however the policy of Canterbury DHB to regularly examine information, or to unreasonably intrude on the personal affairs of staff. Where such examination is required, senior management authorisation shall first be sought.

Monitoring of Information Systems

Canterbury DHB information systems may be subject to monitoring for security, network management, and inappropriate use purposes.

Records of information system access and use, including Internet Web sites, may be kept.

Personal Use of Information Systems

Canterbury DHB owns and operates information systems and IT equipment which are provided for use by employees in support of organisational activities. The systems and equipment are subject to cost, capacity and performance restraints.

Personal or non-business use, whilst permitted, must be incidental and occasional, performed in a reasonable and responsible manner, and in accordance with the policies detailed in this document. If there are unreasonable cost or performance implications associated with personal or non-business use, Canterbury DHB reserves the right to remove data or access without prior approval.

Violations of Policy

Non-adherence to policy is of serious concern to Canterbury DHB as it can result in confidential or sensitive Canterbury DHB or patient information being compromised.

Violation of the policies may be grounds for disciplinary procedures in accordance with the Canterbury DHB Code of Conduct and Disciplinary Action policies. It can also lead to revocation of system access and privileges, and to restoration of systems to which unauthorised equipment or software has been added, to their original state.

Approved Non-Compliance

Where a particular policy cannot be complied with for a substantive business reason, or where it can be demonstrated that a lesser control does not create a security exposure, approval for a variation from policy should be sought from the Information Security Manager or Chief Information Officer (CIO).

Variations from policy must be supported by the relevant senior manager/clinician, who must agree in writing to accept any associated risk.

A record of approved variations shall be kept and reviewed regularly by the Information Security Manager.

Accreditation

Information management and security are important aspects on the Quality Health New Zealand Accreditation Programme. The implementation of adequate protective measures in accordance with Information Security policies is a key measurement area.

In addition, information security management system certification, based on standard AS/NZS ISO/IEC 17799:2001, is available from the Joint Accreditation Service – Australia and New Zealand (JAS-ANZ).

Associated documents

CDHB documents, e.g.

- CDHB Manual, Volume 2 - Legal and Quality
  Informed Consent
- Burwood Hospital Manual, Volume C - Health and Safety
  Hazard Identification
- Related procedure documents, if any
- Relevant external documents

Policy statement

The objectives of the Canterbury DHB Information Security Policy are to:

- Protect Canterbury DHB information assets, patient records and other confidential and sensitive information, from accidental or intentional disclosure, damage, modification, denial of use, or total or partial loss.
- Safeguard Information Technology (IT) resources and equipment from unauthorised access and use.
- Acquaint Canterbury DHB management and staff with information security risks and provide guidelines to assist in minimising or eliminating these risks.
- Clarify responsibilities and duties, and highlight individual employee accountability, in respect to the protection of Canterbury DHB information assets, patient records and other confidential and sensitive information.
- Establish a basis for the assessment and audit of security controls.

Health Intranet of New Zealand General Security Policy

The Health Intranet, of which Canterbury DHB is a founding member, has been developed as a New Zealand-wide electronic health network to assist the delivery of integrated healthcare.

A separate security policy document has been issued by the Health Intranet Governance Board. Copies can be obtained from the Canterbury DHB Information Security Manager.

Canterbury DHB users of the Health Intranet are bound by both the Health Intranet and Canterbury DHB Security Policies.

Policy Owner	Chief Information Officer
Policy Authoriser	Chief Medical Officer
Date of Authorisation	31 August 2015

Privacy policy

Contents

The latest version of this document is available on the CDHB intranet/website only.

Printed copies may not reflect the most recent updates.

Policy

All staff and others to whom this policy applies will comply with Canterbury DHB's legal and ethical obligations concerning patient privacy and confidentiality.

Purpose

The purpose of this policy is to ensure the protection of individual privacy within the Canterbury DHB and to ensure that the Canterbury DHB meets its obligations pursuant to the Privacy Act 1993 and the Health Information Privacy Code 1994.

Scope/Audience

This policy applies to:

- All staff employed by Canterbury DHB.
- All visiting health professionals and students undertaking training or education within the organisation.
- All Canterbury DHB volunteers.
- All independent practitioners contracted to provide patient care.
- All contractors with Canterbury DHB, i.e. cleaners, security guards, etc.

Associated documents

- Health Information Privacy Code 1994.
- Health Act 1956.
- Privacy Act 1993.
- Official Information Act 1982.
- Code of Health & Disability Services Consumers' Rights.
- Canterbury DHB Manual, Volume 2 - Legal and Quality
- -Release of Patient Information Policy.
- Canterbury DHB Manual, Volume 11 - Clinical

  - Informed Consent Policy
- Canterbury DHB Manual, Volume 3 - Human Resources
  - Employee Health Information Policy.

1 Introduction

The accumulation of details about a person's health, disabilities or treatment constitutes information of the greatest sensitivity.

During the course of carrying out their day to day activities all staff and others who come on to a hospital site will come into contact with confidential information. All such individuals have ethical, legal and contractual obligations to uphold and observe patient confidentiality.

All staff and others to whom this policy applies should familiarise themselves with the Health Information Privacy Code 1994. A full copy of this Code is available from the Patient Information Office, any Privacy Officer or Corporate Legal.

The Health Information Privacy Code is a Code of practice issued by the Privacy Commissioner pursuant to the Privacy Act 1993. The Code is specific to the health industry and regulates how we deal with the health information concerning our patients.

1.1 Privacy Officers

The CanterburyDHB has a Corporate Privacy Officer who is also the Senior Corporate Solicitor.

The roles and responsibilities include:

- Protect and promote individual privacy by encouraging compliance with the Code.
- Deal with requests for information.
- Work with the Privacy Commissioner on any investigations; and;
- Otherwise ensure compliance with the Act and The Code.

Other Privacy Officers in the Canterbury DHB are:

- Corporate Solicitor
- Patient Information Team Leader, Christchurch Hospital
- Customer Services Manager, Christchurch Hospital
- Medical Records Officer - Mental Health Services
- Customer Services Co-ordinator, Older Persons Health TPMH, Specialist Mental Health Services and Community Dental Services

2 Health Information Privacy Code 1994 ("The Code")

2.1 General Policy

The Health Information Privacy Code applies to everyone working in the health sector who handles health information. The Code sets out 12 rules which provide a framework for the management of personal health information. The rules are interlinked, so that policies concerning collection of information can affect what happens when it is disclosed. Some rules set out a principle, then provide exceptions to it.

The Code co-exists with ethical obligations. It does not override them, and ethical obligations do not override the Code. Health professionals must comply with the Code and with their professional code of ethics.

2.2 Information Covered by the Code

The Code covers health information about an identifiable individual (even if they are deceased), including information about:

- a person's health or disabilities;
- a person's medical history;
- any health or disability services provided to someone;
- patients, which is collected while providing health and disability services to them. This might include collecting addresses or information relevant to a subsidy entitlement.

2.3 Meaning of "Representative"

The term "representative" is frequently used in the Code.

It means:

- When a person is dead – the executor or administrator of their estate. (The person dealing with a deceased's assets in accordance with their Will.)
- Where a person is under 16 – a parent or guardian.
- Where neither the above apply but the person is unable to give consent or exercise his or her rights – someone who seems to be lawfully acting on the person's behalf or in his or her interests.

3 Rule 1 – Necessity and Purpose

The Canterbury DHB must not collect health information unless that information is collected for a lawful purpose connected with a

function or activity of the Canterbury DHB and the collection is necessary for that purpose.

Consequently, the Canterbury DHB must not collect superfluous information to that required to treat a patient. Information such as a patient's income, sexual orientation, marital status etc should not be collected unless it is necessary in order to provide care and treatment to that patient.

4 Rule 2 – Information Should Be Collected From the Patients Themselves

Generally, information about patients should be collected from those patients. However, Rule 2 lists a number of exceptions to this general principle, such as:

- Where the patient has authorised collection from someone else.
- Where collecting information from patients would prejudice their interests, prejudice the purpose of collection, or prejudice the safety of any person.
- Where collecting the information from the patient is not reasonably practicable.

An example of when Rule 2 may apply is when family members accompany a patient. Often family members will be anxious to advise a health professional of the nature of an injury or the symptoms of an illness but they may not have an accurate understanding of the nature of the injury or illness. Health professionals should always try to obtain information (in the first instance) from the individual concerned and should verify with the patient if possible, information collected from another source.

5 Rule 3 – Steps to be Covered When Collecting Information

Where information is collected directly from patients, the Canterbury DHB must take reasonable steps to ensure they are made aware of a number of matters, including:

- That information is being collected - this is not always obvious, e.g. if video or audio recording is used.
- The purpose of collection, i.e. if personal non health information is required for completing ACC forms etc, the Canterbury DHB must explain why that information is being collected.
- The intended recipients of the information - there is no need to list every possibility but a general indication should be given.

- The consequences of not supplying the information - i.e. a particular treatment may not be able to be given or a subsidy applied for.
- The patient's rights of access to their information and right to request a correction given by Rules 6 and 7 of the Code (refer pages 38 and 48).

Exceptions to fulfilling Rule 3 requirements include:

- The patient has authorised the Canterbury DHB not to do so.
- Compliance by the Canterbury DHB would prejudice the interests of the patient or prejudice the purposes of collection, e.g. interaction charts in Child Protection Cases.
- Compliance is not reasonably practicable in the particular circumstances, i.e. it would delay emergency treatments.

If it is not practicable to give an explanation when the information is collected, it should be done as soon as practicable afterwards.

6 Rule 4 - Manner of Collection

Health information may not be collected by unlawful, unfair or unnecessary intrusive means.

For example, a receptionist may ask patients a number of questions for their records upon arrival at a clinic. Consideration should be given as to whether the patient can fill in a form or verify existing written information rather than verbally give personal details in a waiting area where other patients can overhear.

While it is acknowledged that given the space limitations within hospitals it may not always be possible to ensure physical privacy, consideration should be given as to the steps that can be taken to maximise privacy.

7 Rule 5 - Security Safeguards

Rule 5 of the Code requires the Canterbury DHB to take reasonable security safeguards against:

- loss of patient information.
- access, use, modification or disclosure of patient information, without Canterbury DHB's authority.
- other misuse.

Refer page 9 for best practice guidelines.

An example of how this Rule may apply is in reception areas where sometimes mail is kept (in readiness for collection) on public counters where it can be read by others. In compliance with this Rule, it should be removed from public view. Likewise, a trolley full of medical records should not be left unattended where the public has access.

8 Rule 6 - Right of Access to Personal Information

(Refer also to Canterbury DHB's Release of Information Policy)

People have a right to access information about themselves. This right is given by rule 6 of the Code .

The Right to access is important both from a privacy perspective and from a treatment perspective. Several of the rights in the Code of Health and Disability Services Consumers' Rights are concerned with the communication of information and with Informed Consent. So, when considering a patient's request for personal health information, the Canterbury DHB should consider whether a refusal would hinder the patient's ability to give informed consent to a procedure.

The request to view or have a copy of personal information may be verbal or written. Proof of identification is required for all requests.

Requests for copies of patients' records should be directed to the Patient Information Office at Christchurch Hospital or the appropriate Privacy Officer.

The Canterbury DHB must not charge for making information available in response to a request from the Patient to whom the information relates.

Information may only be withheld if the withholding falls within one of the exceptions in the Code. Some of the common exceptions include:

- Release of the information would be likely to prejudice the maintenance of the law.
- Release of the information would be likely to endanger the safety of an individual.
- Release would involve the unwarranted disclosure of the affairs of another individual or a deceased individual.
- Release would be likely to prejudice the physical or mental health of the requestor.

For an overview of the steps to be taken in providing access to patient notes refer to Canterbury DHB's Release of Information Policy.

9 Rule 7 – Requests for Corrections

People have the right to ask for their health information to be corrected.

If the Canterbury DHB is not willing to make a correction, it must, if requested, take reasonable steps to attach a statement of the correction sought, but not made. The statement must be attached so that it will always be read with the disputed information.

When a patient disagrees with a diagnosis and wants it removed from the file, careful consideration must be given before altering the original record. Removing the disputed diagnosis could render the notes incomplete. If it is acknowledged that a diagnosis is wrong this should be recorded alongside the original entry.

The Canterbury DHB is required to provide reasonable assistance to any individual wishing to record a statement of correction.

10 Rule 8 – Accuracy

Before using information, the Canterbury DHB must take reasonable steps to ensure information is:

- correct
- up to date
- complete
- relevant
- not misleading.

This can be particularly important where information has been obtained from a source other than the person concerned.

11 Rule 9 – Keeping Health Information

The CDHB policy for disposal of clinical records requires information to be retained for 10 years following death of the patient.

12 Rule 10 – Using Information

Information obtained in connection with one purpose must not be used for any other purpose unless the use falls within one of the exceptions of Rule 10.

Rule 10 does allow uses which are "directly related" to the purpose for obtaining the information. For instance, information obtained for care and treatment may also be used for administrative purposes related to that care and treatment.

Some of the exceptions to Rule 10 include using information for another purpose if it is necessary to prevent or lessen a serious threat to public health or public safety or health of an individual.

13 Rule 11 – Disclosure of Information

This Rule is dealt with in its entirety in the Canterbury DHB Release of Information Policy. Please refer to that policy when dealing with disclosure of information.

14 Rule 12 – Unique Identifiers

This Rule states that the Canterbury DHB must not assign a unique identifier to an individual unless the assignment of that identifier is necessary to enable the Canterbury DHB to carry out one or more of its functions efficiently. Further, the Canterbury DHB must not assign to an individual a unique identifier that, to the Canterbury DHB's knowledge, has been assigned to that individual by another entity.

A unique identifier is defined as an Identifier:

Measurement/Evaluation

How this policy will be measured on how it is used, e.g. an audit.

- That is assigned to an individual by an agency for the purposes of the operations of the agency; and
- That uniquely identifies that individual.

15 Rule 12 expressly excludes the NHI number which can be used.

The reasoning behind this Rule is the concept that individuals should not be “labelled” or identified as belonging to a particular group such as "bad payers” for example.

16 Privacy – Recommended Best Practice

16.1 Office/Reception/Areas

- Clinical records should not be kept in places easily accessible by the public and unrelated staff.
- Patients should not be asked to verify personal details in reception/waiting areas where they can be overheard by others.
- Outgoing mail awaiting collection should not be left where it can be seen.
- All computers should be placed so that PC screens cannot be read except by staff entitled to the information. Screen savers should be used.
- Any correspondence, old labels or other documentation containing patient information authorised to be discarded must go in the blue security bins to be shredded.
- Care must be taken that operation lists, clinic lists or any other administrative forms containing patient information are not left in any place accessible to the public.
- Operation or clinic lists should not be left in consultation rooms where they can be seen by other patients.
- Offices and filing cabinets should be locked when unattended.
- Names and details of patients should not be discussed in lifts or other public places.

17 Clinical Records

- All clinical records being transported by hospital staff or through the mail system within hospitals must be suitably covered and secured.
- If clinical records are being carried through a public area, they should be carried in an envelope, if possible, or at least, with the patient’s name unable to be viewed.
- Trolleys containing clinical records should not be left in areas accessible to the public or other patients.
- Except where necessary, records should not be left at the patient's bedside unless the patient has consented.

- Only those staff members involved in the care and treatment of a patient may have access to that person's clinical records.
- Clinical records should not be transported off-site unless off-site storage is required or is absolutely necessary. If so, they should not be left uncovered in a vehicle which must remain locked at all times.

17.1 Identity of Patients

- Wherever possible, patients should be asked on admission to the ward areas if their name can be displayed on room doors, above beds and on name boards.
- Ideally name boards in wards/units should not be able to be viewed by any members of the public.
- Name boards should only show patient name, room allocation and who is responsible for their care.
- Patients can request that no details be released in relation to their condition.
- Unless specific consent is given, only the general condition of a patient, (e.g. satisfactory) can be released.
- If at all possible, patients should not be asked to verify personal details in waiting rooms/ward areas where they can be overheard.
- When requesting information from a patient, all care should be taken to ensure that this is achieved in a manner that respects the individual's privacy.
- Patient's consent must be obtained if a photograph is to be taken of them and such consent must be in writing if the photograph is to be used for educational or research purposes. (Please refer to the Canterbury DHB Informed Consent Policy.)

17.2 Facsimiles and emails

Sending faxes or emails that contain information about patients should be avoided unless necessary, or a dedicated fax line is used.

When a fax or email is necessary, staff should:

- Check the number / Address of the recipient.
- Check the number / Address before sending.
- Where practicable, telephone prior to sending so the recipient is aware it is being sent.
- Fax machines should be placed in rooms that can be secured after hours.

- Fax machines should be placed in areas where the public are unable to access information coming through.
- All faxes/emails sent should have a disclaimer attached, which contains one of the following:

"Caution: The information contained in this facsimile is confidential. If the reader is not the intended recipient, you are hereby notified that any use, dissemination, distribution or reproduction of this message is prohibited. If you have received this message in error, please notify us immediately."

"This email and attachments have been scanned for content and viruses and is believed to be clean. This email or attachments may contain confidential or legally privileged information intended for the sole use of the addressee(s). Any use, redistribution, disclosure, or reproduction of this message, except as intended, is prohibited. If you receive this email in error, please notify the sender and remove all copies of the message, including any attachments. Any views or opinions expressed in this email (unless otherwise stated) may not represent those of Canterbury District Health Board.

17.3 Answer Phones

- Leaving messages about or for patients on their answer phones should be avoided.
- When urgent contact is to be made the only message that is acceptable is to leave the telephone number and name for the person to phone back.
- Under no circumstances should the name of the organisation, the clinical area, or reference for any health care treatment be made.

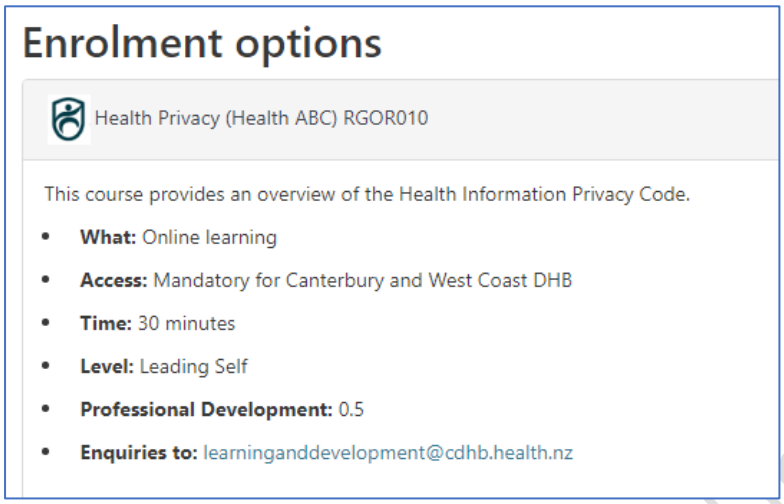
17.4 General

- Patient details should be checked with the individual concerned to confirm accuracy and that the details are up to date before use.
- Information obtained from third parties should be verified with the patient before use.
- Patients should not be stopped in lifts, corridors or public places and their care discussed.
- Wherever practicable an explanation should be given before information is collected as to its intended use and to whom it may be disclosed.

- Information disseminated to patients and members of the public such as the Patient Information Booklet should specify to whom information may be released and why.

Policy Owner	Corporate Privacy Officer
Policy Authoriser	Executive Management Team
Date of Authorisation	27 November 2013

Appendix f - Health Privacy module (in the minimum, screenshots)



healthLearn is the CDHB and WCDHB Learner Management System i.e., our digital platform up which sits all our on-line courses. It's the place where people enrol into courses, have their learning attendance recorded, and complete course participation.

Disciplinary Policy

Purpose

This Policy sets out the Canterbury District Health Board and West Coast District Health Board (referred to as **our** or **we**) approach towards disciplinary matters.

Policy

We are committed to providing a safe workplace for all our people.

In order to do so, we recognise that there are minimum standards of behaviour and performance (**minimum standards**) that our people must meet. Behaviour includes how we interact with others, how we manage ourselves and how we perform at work. Meeting these minimum standards will ensure:

- the morale and productivity of our people is maintained; and
- the safety of our people or patients or visitors is not compromised.

Failing to meet minimum standards may lead to our people receiving disciplinary action up to and including dismissal in line with this policy.

Use of this policy is the most serious action we can take and should only be considered where informal action has been ineffective and/or the breach or surrounding circumstances makes informal action inappropriate.

1. Minimum Standards of Behaviour

Our minimum standards are set out in our Policies and Procedures, particularly our *Our Code of Conduct*. Common reasons for a disciplinary process are breaches/alleged breaches of the Code of Conduct. A breach of our minimum standards may be found to amount to misconduct or serious misconduct.

1.1 Misconduct

Misconduct involves a breach of our minimum standards which alone isn't of the severity to warrant dismissal.

1.2 Serious Misconduct

Serious misconduct involves a breach of our minimum standards which seriously undermines the relationship of trust and confidence and therefore alone may be of the severity to warrant dismissal.

2. Suspension

Suspension is the removal of one of our people from the workplace while a disciplinary process is undertaken, and is not, of itself, disciplinary action. Where suspension is being considered, People and Capability should be consulted.

We may suspend one of our people where the alleged breach of minimum standards is sufficiently serious and/or is warranted to protect the health and safety of our people, patients or visitors.

In most circumstances, suspension will be on full pay and the suspended person must remain available and contactable in order to participate in the disciplinary process and address matters that may arise.

3. Disciplinary Principles

Where there is behaviour that may not meet our minimum standards, a process to identify what has happened (findings of fact) will be undertaken before any disciplinary action is taken.

Disciplinary action may include a written warning, final written warning or dismissal.

3.1 Warnings

We have two types of warnings in instances of misconduct or serious misconduct:

- Written warning; and/or
- Final written warning.

The type of warning will reflect the seriousness of the situation and does not necessarily need to be graduated. For example, one of our people may be given a final written warning without having previously received a written warning.

Graduated warnings may be given in instances where the misconduct or serious misconduct is of a similar or dissimilar nature.

Regardless of the level of the warning, all warnings will:

- Be written and placed on the person's employee file;
- State the duration, being up to 12 months from the date of the communication of the disciplinary action; and
- State what will happen if minimum standards of behaviour are not met in the future.

3.2 Dismissal

A decision to dismiss is the most serious form of disciplinary action and can happen in instances of repeated misconduct or serious misconduct.

Dismissal may be preceded by a graduated warning process however where serious misconduct has been proven, dismissal may occur in the absence of any prior warnings. Dismissal may occur with or without notice.

4. Professional Obligations

We may have an obligation to inform the responsible registering authority when one of our people who is a health practitioner is subject to a disciplinary process, resigns and/or is dismissed.

Applicability

This Policy applies to all our employees, contracted individuals, volunteers, visiting health professionals and students (referred to as **our people**).

Roles and Responsibilities

During the disciplinary process, the following principles of fairness must be adhered to.

Our people must be:

- Reminded of the minimum standards expected of them in their employment;
- Advised in writing about the issue being investigated and/or the allegation/s made against them;
- Given an opportunity and reasonable time to prepare and present their response, including supporting material;
- Provided with relevant information, subject to the provisions of the Privacy Act 1993;
- Given an opportunity to have representation;
- Allowed to present material or information to support their case; and
- Advised of the consequences or possible consequences arising out of a disciplinary process and/or noncompliance with any remedial action determined at the end of a disciplinary process.

We must:

- Act fairly and reasonably in conducting any disciplinary process;
- Ensure that disciplinary action is taken in line with principles of fairness, reasonableness and consistency; and
- Act in the disciplinary process within appropriate authorities.

Policy measurement

We will measure the number of disciplinary outcomes issued, up to and including dismissal. This will be reported annually. All data will be reported anonymously to preserve the privacy of our people.

Associated material

Including, but not limited to:

Our DHBs

- Doing the Right Thing – Our Code of Conduct
- Maintaining a Bullying, Harassment and Discrimination Free Workplace Policy
- Diversity and Inclusion Policy
- Guidelines and Flowcharts on Max

References

- Employment Relations Act 2000
- Privacy Act 1993

Contents