

Policy: A 'Just Culture'

Purpose

The purpose of this policy is to improve patient safety at CM Health. Staff should feel safe and supported when voicing concerns about issues regarding their own actions or those in the environment around them. This includes feeling able to report incidents of patient harm without fear of reprisal. Furthermore a just culture signals that such incidents will be investigated in a way that the underlying systemic failures are identified and rectified, rather than apportioning individual blame. In this way the just culture supports improved patient safety.



Note: This policy must be read in conjunction with CM Health policies; [Open Disclosure with Patients Policy](#), [Incidents Process and Resolution Policy](#) and the [CMDHB code of conduct](#)

Scope

This policy is applicable to all CM Health employees (full-time, part-time and bureau), contractors, visiting health professionals and students working in any CM Health facility.

CM Health principles of a just culture

- Acknowledges that first and foremost CM Health staff strive to deliver ever safer and more effective care
- Constructive criticism which is offered in good faith, with the intention of improving patient care or patient advocacy, is appropriate professional behaviour
- CM Health commits to holding individuals accountable for their own performance in accordance with their job responsibilities and our core value of care and respect for both patients and other staff. However, individuals should not carry the burden for system flaws over which they had no control.
- A fair and just culture organisation is one that learns and improves by openly identifying and examining its own weaknesses.
- CM Health will act to improve patient safety by implementing change based on our analysis of adverse events and potential patient harm, and is committed to assigning responsibility for implementing identified actions to specific individuals or groups.
- CM Health will inform patient and family members, healthcare providers, leadership and Board members about actions that have been taken to improve patient safety.

Document ID:	A13187	CMH Revision No:	1.0
Service :	Risk Management and Quality Assurance	Last Review Date :	09/12/2017
Document Owner:	Deputy Chief Medical Officer (CMO) and Clinical Director	Next Review Date:	09/12/2020
Approved By:	Clinical Governance Group (CGG)	Date First Issued:	15/02/2010
<i>If you are not reading this document directly from the Document Directory this may not be the most current version</i>			

A Just Culture and incident reporting:

A fair and just culture means applying a systems approach to the investigation of patient harm. This approach recognises that all individuals are error prone and that the optimum way to improve patient safety and learn from adverse events, is through staff feeling safe to voice their concerns, report errors and to investigate the underlying causes of such errors. A Just Culture policy means fair-minded treatment, having productive conversations, and creating effective structures that encourage people to reveal their errors and help the organisation learn from them.

- Building a culture of trust that supports transparent and open communication
- Establishing a supportive work environment where learning from experience is valued, and lessons and best practice are shared
- Ensuring staff are familiar with their role and the roles of others regarding incident and accident reporting
- Promoting systems thinking with an understanding of active and latent system failures; a commitment to a transparent investigation process to identify these failings; and a commitment to improve the underlying system weaknesses that contributed to patient harm
- Actively support the implementation of corrective actions of system weaknesses and risk mitigation activities
- Promptly escalating incidents of actual or potential harm where there is significant risk to patients and/or the organisation

It recognises:

- Adverse events are frequently the result of inadequate systems or complex system errors
- Despite best efforts of competent and caring professionals adverse events occur
- Blaming individuals does not improve patient safety and may harm organisational learning from errors

A Just Culture and professional behaviour:

- Upholding standards of respectful behaviour as a core CMDHB value.
- Holding staff to account when they display intimidating or disruptive behaviour that undermines patient safety activities
- Establishing and supporting an organisational procedure to address intimidating and/or disruptive behaviours

Intimidating and disruptive behaviours in healthcare organisations can contribute to medical errors, poor patient satisfaction, preventable adverse outcomes, and increase the cost of care and staff turnover.¹ The A Just Culture policy is supported by CM Health’s shared values which underpin the organisation’s expectations of every employee’s behaviour. Patient safety and performance of the health care team are improved by every

¹ The Joint Commission. Sentinel Event Alert, issue 40, July 9 2008. www.jointcommission.org.

Policy Number:	A13187	Version:	1.0
Department:	Middlemore Central	Last Updated:	9/05/2014
Document Owner:	Clinical Director Patient Safety Quality Assurance	Next Review Date:	9/05/2017
Approved by:	Clinical Governance Group	Date First Issued:	15/02/2010
Counties Manukau Health			

employee consistently behaving in accordance with organisational values of Care & Respect, Teamwork, Professionalism, Innovation, Responsibility and Partnership.

Responsibilities:

All Employees:

All employees of CM Health are expected to share in the commitment to the A Just Culture policy and are expected to contribute through:

- Supporting the principles of a just culture
- Upholding the standards of respectful behaviour as a core CM Health value
- Taking a systems approach to errors and focusing on the “how and why” of an incident or accident
- Ensuring they are familiar with their role and the roles of others in regards to reporting incidents, accidents and near misses
- Encouraging and supporting their colleagues and other staff members to report incidents and near misses
- Actively participating in investigations of incidents and near misses if required/requested
- Promptly escalating incidents or accidents of actual or potential harm where there is significant risk to the organisation

Management/Leadership:

“It is the responsibility of Leaders to support the consistent delivery of “Just Culture” behaviours. Also the organisation has a responsibility to provide the learning and development required to make such a culture happen.” Geraint Martin CEO (2009)

Exclusions

This policy does not apply when incidents occur as the result of an intentionally unsafe act involving the following:

1. A criminal Act
2. The use of illicit drugs or alcohol
3. A deliberate unsafe act
4. Deliberate patient harm

Intentionally unsafe acts are dealt with through avenues other than those defined in this policy.

Policy Number:	A13187	Version:	1.0
Department:	Middlemore Central	Last Updated:	9/05/2014
Document Owner:	Clinical Director Patient Safety Quality Assurance	Next Review Date:	9/05/2017
Approved by:	Clinical Governance Group	Date First Issued:	15/02/2010
Counties Manukau Health			

Associated Documents

Other documents relevant to this policy are listed below:

NZ Legislation	Code of Health and Disability Services Consumers' Rights Regulation 1996
CMDHB Clinical Board Policies	Incidents Process and Resolution Policy Open Disclosure with Patients – Policy Code of Conduct – Policy

References (Evidence Based Practice)

The Joint Commission. Sentinel Event Alert, issue 40, July 9 2008.
www.jointcommission.org.

Marx, David: Patient Safety and the “Just Culture”: A Primer for Health Care Executives (2001)

Institute of Medicine: To Err is Human: Building a Safer Health System (1999)

Dana-Farber Cancer Institute: Principles of a Fair and Just Culture (IHI Patient Safety Officer Program 2009)

Connor M, Duncomb D, Barclay E et al. Creating a Fair and Just Culture: One institutions path toward organisational change. The Joint Commission Journal on Quality and Patient Safety. 2007; 33: 617-624

Frankel AS, Leonard MW, Denham, CR. Fair and Just Culture, Team Behaviour and Leadership Engagement: The tools to achieve high reliability. Health Services Research 2006; 41 (4) Part II. 1690-1708

Fair and Just Culture, Team Behaviour and Leadership Engagement: The tools to achieve high reliability. Frankel, A et al. Health Services Research 2006; 41 (4) Part II. 1690-1708

Term/Abbreviation	Description
--------------------------	--------------------

Policy Number:	A13187	Version:	1.0
Department:	Middlemore Central	Last Updated:	9/05/2014
Document Owner:	Clinical Director Patient Safety Quality Assurance	Next Review Date:	9/05/2017
Approved by:	Clinical Governance Group	Date First Issued:	15/02/2010
Counties Manukau Health			

released under Official Information Act ref OA 23062020 Van Wey Lovatt

Incident	An event or circumstances which could have, or did, result in: <ul style="list-style-type: none"> • Unintended or unnecessary harm to a person • And/or complaint • Loss or damage
Adverse Event	An incident that has resulted in unanticipated death or major loss of function not related to the natural course of the consumer's illness or underlying condition.
Root Cause Analysis (RCA)	A systematic repetitive process whereby the factors that contribute to an incident are identified by reconstructing the sequence of events and repeatedly asking "why?" until the underlying root causes have been determined.

released under Official Information Act - ref OIA 23062020 Vanja Lovatt

Policy Number:	A13187	Version:	1.0
Department:	Middlemore Central	Last Updated:	9/05/2014
Document Owner:	Clinical Director Patient Safety Quality Assurance	Next Review Date:	9/05/2017
Approved by:	Clinical Governance Group	Date First Issued:	15/02/2010
Counties Manukau Health			

Policy: Code of Conduct

Overview

Abstract This document outlines the standards of behaviour and performance expected of our employees in order to achieve CMDHB's Vision and Values.

Contents This document contains the following topics:

Topic	See Page
Introduction	2
Guidelines.....	3
Reference Information	5

Document ID:	A5701	CMH Revision No:	1.2
Service :	N/A - Controlled document used across the organisation	Last Review Date :	14/02/2019
Document Owner:	Director - Human Resources	Next Review Date:	14/06/2019
Approved by:	Executive Leadership Team (ELT)	Date First Issued:	30/09/2000
Counties Manukau Health			

If you are not reading this document directly from the Document Directory this may not be the most current version.

Introduction

Purpose The purpose of this document is to formally document CMDHB's expectations of employee standards of behaviour and performance. Appropriate performance and behaviour of employees has a major influence on positive outcomes for patients, other employees and the community we serve.

Scope The contents of this document apply to all dealings between CMDHB and its employees.

Document ID:	A5701	CMH Revision No:	1.2
Service :	N/A - Controlled document used across the organisation	Last Review Date :	14/02/2019
Document Owner:	Director - Human Resources	Next Review Date:	14/06/2019
Approved by:	Executive Leadership Team (ELT)	Date First Issued:	30/09/2000
Counties Manukau Health			

If you are not reading this document directly from the Document Directory this may not be the most current version.

Guidelines

Code of Conduct Guidelines

We expect an appropriate standard of conduct from you. This means:

- Performing your tasks well, and fulfilling your responsibilities to the required standards
- Behaving in accordance with our shared values.

CMDHB is committed to resolving employee problems as early as possible and ensuring that fairness is a key principle.

All those with responsibility for leading and supervising others must ensure that their people:

- Know what is expected of them and to what standard
- Are given adequate training, advice and counselling to enable them to reach that standard
- Receive adequate training and supervision when required to perform a new task
- Are informed promptly of any areas for improvement or correction
- Are given every reasonable opportunity to improve their performance.

It is the responsibility of CMDHB to address performance problems, and for the employee to respond by helping to identify the reasons for the performance problem(s) and making every effort to improve.

If performance problems arise, coaching, training or counselling may be required: a two-way dialogue to reflect shared responsibility for achieving required performance.

If this is unsuccessful, the disciplinary process may be invoked. Misconduct, poor performance or inappropriate behaviour will need prompt intervention.

Continued on next page

Document ID:	A5701	CMH Revision No:	1.2
Service :	N/A - Controlled document used across the organisation	Last Review Date :	14/02/2019
Document Owner:	Director - Human Resources	Next Review Date:	14/06/2019
Approved by:	Executive Leadership Team (ELT)	Date First Issued:	30/09/2000
Counties Manukau Health			

If you are not reading this document directly from the Document Directory this may not be the most current version.

Guidelines, Continued

Types of Intervention

The normal forms of intervention are:

- Counselling and/or team involvement
- Formal statement of expectations and consequences
- Redeployment into a position carrying less responsibility/ or transfer/ or restructuring of current position
- A sequence of Warnings, or a Final Warning if appropriate
- Termination with notice or summary dismissal

Employees should familiarise themselves with the Discipline and Dismissal Policy, which gives examples of misconduct, serious misconduct and poor performance. The policy is available on our Intranet.

Document ID:	A5701	CMH Revision No:	1.2
Service :	N/A - Controlled document used across the organisation	Last Review Date :	14/02/2019
Document Owner:	Director - Human Resources	Next Review Date:	14/06/2019
Approved by:	Executive Leadership Team (ELT)	Date First Issued:	30/09/2000
Counties Manukau Health			

If you are not reading this document directly from the Document Directory this may not be the most current version.

Reference Information

Related documents

Other documents relevant to this policy/process/procedure are listed below:

Type	Title
NZ Legislation	<ul style="list-style-type: none"> • Employment Relations Act (2000) • Race Relations Act (1971) • Human Rights Act (1993) • Treaty of Waitangi
CMDHB Policy / Procedure	<ul style="list-style-type: none"> • Discipline & Dismissal Policy • Discipline & Dismissal Procedure • Recruitment • Tikanga Best Practice Policy • Harassment Prevention Policy • Code of Conduct for CMDHB Board and Committee Members Policy • Engagement of Contractors and Consultants Policy
Other	CMDHB Vision and Values

I,.....(full name) have read and agree to comply with the above expected standards of behaviour and performance.

.....
Signature

.....
Date

Document ID:	A5701	CMH Revision No:	1.2
Service :	N/A - Controlled document used across the organisation	Last Review Date :	14/02/2019
Document Owner:	Director - Human Resources	Next Review Date:	14/06/2019
Approved by:	Executive Leadership Team (ELT)	Date First Issued:	30/09/2000
Counties Manukau Health			

If you are not reading this document directly from the Document Directory this may not be the most current version.

Policy: Bullying and Harassment Prevention and Response

Purpose

The purpose of this policy is to provide:

- clear statements regarding Counties Manukau Health's zero tolerance towards workplace harassment, bullying and discrimination
- an overview of the processes for reporting of and dealing with harassment, bullying or discrimination allegations or concerns.

Scope

This policy is applicable to all Counties Manukau Health employees, contractors and volunteers and deals with real and perceived instances of employee-to-employee harassment, bullying or discrimination.

It covers all bullying and harassment behaviours that happen:

- in the workplace
- between work associates, for example on social media, or any social or professional work situations
- during work events such as conferences, training and work-based activities
- outside the workplace if it is in the context of the employment relationship or affects the workplace.

Note:

Instances of patient/public harassment of employees in the workplace are managed through the **Incident Reporting** process.

Instances of employee harassment of patients or members of the public in the workplace are managed through the **Complaints and/or Incident Reporting** process.

Sexual harassment will be covered specifically by the Sexual Harassment Prevention and Response policy.

Introduction

Commitment

Counties Manukau Health is committed to a working environment that is friendly, trusting, and free of unwelcome behaviour and abuse of power or position.

Workplace bullying, discrimination, racial or any other forms of harassment are examples of unacceptable behaviour that can occur at Counties Manukau Health.

Document ID:	A5711	CMH Revision No:	6.0
Service :	N/A - Controlled document used across the organisation	Last Review Date :	26/02/2019
Document Owner:	Director - Human Resources	Next Review Date:	26/02/2022
Approved by:	Executive Leadership Team (ELT)	Date First Issued:	29/11/2002
Counties Manukau Health			

If you are not reading this document directly from the Document Directory this may not be the most current version.

Everyone has the right to work in an environment that is free from workplace bullying, discrimination, racial or any other forms of harassment.

Counties Manukau Health will take any concern or complaint of harassment, discrimination or bullying seriously and handle it with sensitivity and impartiality.

Complaints that are upheld may result in disciplinary action being taken against a perpetrator.

Cultural differences

Understanding cultural differences is vital for Counties Manukau Health. What may be acceptable in one culture may be very unacceptable in another.

Counties Manukau Health expects all employees to consider these differences in their interaction with each other.

Definition of Harassment

Harassment is any unwanted or unjustified behaviour that another person finds offensive or humiliating, and because it is serious or repeated it has a negative impact on the person's employment, job performance or job satisfaction.

Harassment may be verbal, physical or other, and may be related to:

- gender
- marital status
- religious belief
- ethical belief
- colour or race, ethnic or national origins
- disability
- age
- political opinion
- employment status
- family status
- sexual orientation.

Racial harassment specifically is uninvited behaviour that humiliates, offends or intimidates someone because of their race, colour, or ethnic or national origin.

Examples of harassment in the workplace are:

Document ID:	A5711	CMH Revision No:	6.0
Service :	N/A - Controlled document used across the organisation	Last Review Date :	26/02/2019
Document Owner:	Director - Human Resources	Next Review Date:	26/02/2022
Approved by:	Executive Leadership Team (ELT)	Date First Issued:	29/11/2002
Counties Manukau Health			

If you are not reading this document directly from the Document Directory this may not be the most current version.

- a generally 'hostile' work atmosphere of repeated put-downs, offensive stereotypes, malicious rumours, or fear tactics
- a general work atmosphere of repeated jokes, teasing, flirting, leering or sleazy 'fun'
- making offensive remarks about a person's race
- personally sexually offensive verbal comments
- repeated comments or teasing about someone's alleged sexual activities or private life
- persistent, unwelcome social invitations, telephone calls or any other form communication technology from workmates at work or at home
- unwelcome physical contact – e.g. patting, pinching, touching or putting an arm around another person's body
- provocative visual material – e.g. posters of a sexual nature.

Definition of Discrimination

Discrimination occurs when someone, or a group of people, is/are treated less favourably than another person or group in the same or similar circumstances, because of a particular characteristic.

Definition of Bullying

Bullying is a persistent misuse of power, whether formal or informal. It is offensive, abusive, intimidating, malicious or insulting behaviour. It makes the recipient or target feel upset, threatened, humiliated, or vulnerable and undermines self-confidence. It has a detrimental effect upon a person's dignity, safety, self-confidence and well-being and may cause them to suffer stress. It can be overt or covert. Bullying can be exercised by anyone in any position in an organisation.

Repeated harassment may be considered bullying.

These behaviours could include although are not limited to the following:

- verbal abuse, belittling or demeaning language/gestures
- unjustified criticism, fault-finding or public humiliation
- intimidation, threats or displays of hostility
- sarcasm, teasing, unwanted jokes
- undermining by spreading malicious rumours or bad-mouthing
- withholding of information required to perform tasks
- unwarranted exclusion or isolation.

Document ID:	A5711	CMH Revision No:	6.0
Service :	N/A - Controlled document used across the organisation	Last Review Date :	26/02/2019
Document Owner:	Director - Human Resources	Next Review Date:	26/02/2022
Approved by:	Executive Leadership Team (ELT)	Date First Issued:	29/11/2002
Counties Manukau Health			

If you are not reading this document directly from the Document Directory this may not be the most current version.

Behaviours not considered to be workplace bullying are:

- one-off occasional instances of forgetfulness, rudeness or tactlessness
- setting high performance standards because of quality or safety
- constructive feedback or legitimate advice or peer review
- issuing reasonable instructions
- frank and honest discussions
- warning or disciplining employees in line with organisational policy.

People may sometimes cause offence or harm unintentionally. A principle of harassment is that it is not the intention, or the behaviour, but the way it is received and the effect it has on the person.

Options for dealing with Harassment, Discrimination or Bullying

Any employee who considers they have been subjected to harassment, discrimination or bullying may take any one or more of the options listed below:

- Employees may approach their manager, Human Resources partner, a trusted person, union or other representative or EAP Services for support and/or advice. Counties Manukau Health also maintains a pool of trained contact people available to assist employees with information and support.
- **Self-help** where the offended person approaches the accused party directly and asks that the behaviour of concern stops
- **Informal interventions** involving a third party to help resolve a situation. These may include facilitated discussion or mediation
- **Formal complaint** (see below)

Principles

The internal complaints process is designed to be:

- **Accessible** – the complaint process is readily available. Employees should talk to the persons mentioned in the section above or find information on Paanui.
- **Fair** - natural justice requires that the accused party is told of the substance of all allegations against them if the matter is to be formally investigated. Putting an allegation does not necessarily require disclosing the identity of the complainant.
- **Confidential** - this means that information about a complaint is only provided to those people who need to know about it.
- **Efficient** - the complaints process should be conducted without undue delay and dealt with at the lowest appropriate level of intervention.

Document ID:	A5711	CMH Revision No:	6.0
Service :	N/A - Controlled document used across the organisation	Last Review Date :	26/02/2019
Document Owner:	Director - Human Resources	Next Review Date:	26/02/2022
Approved by:	Executive Leadership Team (ELT)	Date First Issued:	29/11/2002
Counties Manukau Health			

If you are not reading this document directly from the Document Directory this may not be the most current version.

Making a formal complaint

Any employee may make a formal complaint if they believe they have experienced harassment, discrimination or bullying in the course of their employment.

Counties Manukau Health will treat all formal complaints seriously. A full and fair investigation will be conducted (unless the complaint is reasonably determined to be frivolous, trivial or otherwise insubstantial).

The complainant and accused party will be interviewed along with any named witnesses.

The accused party has the right to be represented. All parties have the right to have a support person present at any meeting or interview involved in the investigation.

The complainant and accused party will be informed of the process of investigation and have the right to view all the documentary evidence and witness statements.

Both parties also have the right to respond and submit a final submission before the investigator assesses the evidence and completes the investigation.

At the completion of the investigation, a final report will be provided to the complainant and accused party explaining the findings and the basis for those findings.

Behaviour that constitutes harassment, discrimination or bullying may be considered as either misconduct or serious misconduct depending upon the seriousness of the behaviour, persistence of the behaviour, and the impact on the complainant.

If an investigation finds substance to a complaint, the matter will then be dealt with under the disciplinary policy and may result in disciplinary action, including the possibility of dismissal, against the accused party.

Malicious, vexatious or false complaints are considered forms of serious misconduct. This does not include complaints that are found to be lacking in sufficient substance.

Confidentiality, Safety and Privacy

The complainant and the accused party will be advised not to attempt to contact each other about the complaint during the process of investigation.

Document ID:	A5711	CMH Revision No:	6.0
Service :	N/A - Controlled document used across the organisation	Last Review Date :	26/02/2019
Document Owner:	Director - Human Resources	Next Review Date:	26/02/2022
Approved by:	Executive Leadership Team (ELT)	Date First Issued:	29/11/2002
Counties Manukau Health			

If you are not reading this document directly from the Document Directory this may not be the most current version.

All parties to a complaint, including witnesses, shall be required to maintain appropriate confidentiality.

It may be appropriate to take interim measures which ensure the complainant and the accused party do not work together until the matter is resolved. This depends on the nature of the complaint and the relationship between the complainant and the accused party.

While the outcomes of an investigation will be provided to the complainant and the accused party, disciplinary outcomes are private and will only be provided to the person concerned.

Roles and Responsibilities

All Employees, Contractors and Volunteers

Are responsible for upholding this policy by:

- ensuring they understand and comply with this policy on their employment or engagement in any services or projects with Counties Manukau Health
- ensuring they do not use bullying, discriminatory or harassing behavior
- refusing to condone, protect or collude with any person who harasses, discriminates against or bullies others
- speaking up when they are subject to or witness to bullying, discriminatory or harassing behaviours. They should seek advice from a Contact Person or other trusted peer or advisor and if appropriate, use an informal approach to resolve the matter or, as appropriate, lay a formal complaint to management or HR.

Managers

Managers are responsible for fostering a positive, respectful culture in which bullying, discrimination and harassment are less likely to occur.

Managers will uphold this policy by:

- ensuring employees know that harassment, discrimination and bullying are unacceptable and will not be tolerated
- taking appropriate corrective action to deal with unacceptable behaviour
- providing leadership and modelling appropriate and professional behaviour in the workplace
- hearing employee concerns and responding promptly, sensitively and confidentially to all situations where unacceptable behaviour is exhibited or alleged to have occurred

Document ID:	A5711	CMH Revision No:	6.0
Service :	N/A - Controlled document used across the organisation	Last Review Date :	26/02/2019
Document Owner:	Director - Human Resources	Next Review Date:	26/02/2022
Approved by:	Executive Leadership Team (ELT)	Date First Issued:	29/11/2002
Counties Manukau Health			

If you are not reading this document directly from the Document Directory this may not be the most current version.

- notifying Human Resources with any concerns about inappropriate behaviour that have been raised with them.

Human Resources

The Human Resources team are available to:

- help managers and employees know about and meet their obligations under the relevant legislation and this policy
- give advice, support and information if an employee believes sexual harassment has occurred at any level of the organisation. Advice will include options available and how the employee may want to proceed.

The Complainant

Counties Manukau Health will ensure that any employee making an allegation of harassment or bullying is treated fairly.

An employee will not be subjected to discriminatory treatment for making an honest allegation.

A complainant is entitled to:

- information on options available to them
- appropriate personal support
- have a support person or representative present at any discussions or interviews
- have all possible steps taken to protect their privacy
- access to Counties Manukau Health's confidential Employee Assistance Programme (EAP)

Accused Party

Counties Manukau Health will ensure that any employee against whom an allegation of harassment is made (the accused party) is treated fairly.

The accused party is entitled to:

- know the name(s) of the complainant(s) and the details of the allegation, including a copy of the written complaint, as soon as possible after the allegation has been made. This ensures they have a fair opportunity to respond to allegations.
- have a support person or representative present during any discussions or interviews (informal or formal) and

Document ID:	A5711	CMH Revision No:	6.0
Service :	N/A - Controlled document used across the organisation	Last Review Date :	26/02/2019
Document Owner:	Director - Human Resources	Next Review Date:	26/02/2022
Approved by:	Executive Leadership Team (ELT)	Date First Issued:	29/11/2002
Counties Manukau Health			

If you are not reading this document directly from the Document Directory this may not be the most current version.

- have all possible steps taken to protect their privacy.
- access Counties Manukau Health's confidential Employee Assistance Programme (EAP).

Contact/Support People

Introduction

Counties Manukau Health maintains a team of trained contact people to provide initial support and advice to employees in the area of harassment, discrimination and bullying prevention and response. This team will be managed by a Co-ordinator who will be a member of the Human Resources Team.

List of contacts

A list of co-ordinator and designated contact people is available from:

- Human Resources
- Occupational Health & Safety
- myHR on Paanui

Role of the co-ordinator

The role of the Co-ordinator is to:

- ensure a pool of trained contact people is maintained
- arrange training for new contact people and refresher training for existing contact people
- facilitate promotion and publicity of harassment, discrimination and bullying policy within CMH
- be a resource for contact people – i.e. policy clarification, provision of information pamphlets etc.
- collate quarterly statistics reports and submit to General Manager Human Resources

Role of the "contact person"

The role of the contact person is to:

- listen non-judgmentally and impartially to anyone who wants to talk about harassment, discrimination or bullying issues
- provide information on workplace bullying, discrimination and harassment, discuss options, and assist enquirers in making informed decisions
- treat all enquiries with the strictest confidence except where there is risk of violence, self-harm or criminal behaviour

Document ID:	A5711	CMH Revision No:	6.0
Service :	N/A - Controlled document used across the organisation	Last Review Date :	26/02/2019
Document Owner:	Director - Human Resources	Next Review Date:	26/02/2022
Approved by:	Executive Leadership Team (ELT)	Date First Issued:	29/11/2002
Counties Manukau Health			

If you are not reading this document directly from the Document Directory this may not be the most current version.

- provide quarterly statistics reports to Co-ordinator (without identifying the persons concerned).

Contact persons do not hold any special authority and are made up of people from all levels of our organisation. They make themselves available voluntarily in addition to their normal duties. Contact persons are not complaints officers, advocates or counsellors.

Additional support people

An employee can, if they wish, involve support people of their choice (e.g. kuia/kaumatua, matai, union or other representative) to support them at any time in addition to, or instead of, the CMH nominated contact people.

Document ID:	A5711	CMH Revision No:	6.0
Service :	N/A - Controlled document used across the organisation	Last Review Date :	26/02/2019
Document Owner:	Director - Human Resources	Next Review Date:	26/02/2022
Approved by:	Executive Leadership Team (ELT)	Date First Issued:	29/11/2002
Counties Manukau Health			

If you are not reading this document directly from the Document Directory this may not be the most current version.

released under Official Information Act - ref OIA 23062020 Van Wey Lovatt

Associated Documents

Other documents relevant to this policy are listed below:

NZ Legislation	<ul style="list-style-type: none"> • Employment Relations Act (2000) • Human Rights Act (1993) • Race Relations Act (1971) • Health and Safety at Work Act 2015
CMDHB Organisational Policies	<ul style="list-style-type: none"> • Health, Safety and Environmental Management • Discipline & Dismissal Policy • Discipline & Dismissal Procedure • Incident Reporting • Family Violence, Elder/Adult Abuse and Neglect Intervention • Manager's Guide: Addressing Concerns or Complaints of Harassment or Bullying. • Sexual Harassment Prevention and Response
Other Related Resources	<ul style="list-style-type: none"> • Worksafe NZ Guidelines 2014 • Wave.org.nz

Document ID:	A5711	CMH Revision No:	6.0
Service :	N/A - Controlled document used across the organisation	Last Review Date :	26/02/2019
Document Owner:	Director - Human Resources	Next Review Date:	26/02/2022
Approved by:	Executive Leadership Team (ELT)	Date First Issued:	29/11/2002
Counties Manukau Health			

If you are not reading this document directly from the Document Directory this may not be the most current version.

Policy: Protected Disclosure

Purpose

The purpose of this policy is to:

1. provide employees of Counties Manukau DHB with the names of persons to whom they can disclose a serious wrongdoing and a process under which disclosure can be made
2. advise employees disclosing serious wrongdoing of the protections available to them (e.g. identity kept confidential, protection from civil and criminal liability)
3. ensure that all serious wrongdoings are investigated appropriately and that specific action is taken to remedy any wrongdoing
4. comply with the Protected Disclosures Act 2000, which requires public sector organisations to have an internal procedure in which employees can disclose serious wrongdoing;
5. ensure that employees are aware of alternative persons/organisations that they can disclose serious wrongdoing to when the internal procedure is not appropriate.

Scope

This document applies to:

- all employees and former employees of Counties Manukau DHB
- any person seconded to Counties Manukau DHB
- any person engaged or contracted under a contract for services to Counties Manukau DHB.

For the purposes of this document the terms ‘employee’ and ‘employees’ include all of the above.

An Explanation of “Serious Wrongdoing”

Definition of Protected Disclosure

A disclosure will be a ‘protected disclosure’ if:

- the information is about serious wrongdoing in or by that organisation; and
- the employee believes on reasonable grounds that the information is true or likely to be true; and
- the employee wishes to disclose the information so that the serious wrongdoing can be investigated; and
- the employee wishes the disclosure to be protected.

Document ID:	A5719	CMH Revision No:	1.2
Service :	Legal and Privacy Services	Last Review Date :	13/02/2019
Document Owner:	Chief legal advisor	Next Review Date:	13/02/2022
Approved by:	Executive Leadership Team (ELT)	Date First Issued:	17/03/2003
Counties Manukau Health			

If you are not reading this document directly from the Document Directory this may not be the most current version.

A protected disclosure can only relate to ‘serious wrongdoing’ as defined below.

Continued...

An Explanation of “Serious Wrongdoing” (continued)

What is a serious wrongdoing

A “serious wrongdoing” includes:

- an unlawful, corrupt, or irregular use of public funds or public resources; or
- an act, omission, or course of conduct that constitutes a serious risk to public health or public safety or the environment; or
- an act, omission or course of conduct that constitutes a serious risk to the maintenance of law, including the prevention, investigation and detection of offences and the right to a fair trial; or
- an act, omission, or course of conduct that constitutes an offence; or
- an act, omission or course of conduct by a public official that is oppressive, improperly discriminatory or grossly negligent or that constitutes gross mismanagement

Example

Examples of serious wrongdoing are:

- a situation where persons responsible to, or who work in relation to, public finance, are corrupt in relation to their use of the finance, or who use the finance in any unlawful way.
- any violent or abusive actions towards other persons that would constitute an offence

A serious wrongdoing is not:

- something that is not unlawful or offensive but which you may not approve of

Not sure?

If you are not sure whether a matter is a serious wrongdoing, you may make a disclosure under this Policy.

The person responsible for your disclosure can determine whether or not the matter is a serious wrongdoing.

Continued...

Document ID:	A5719	CMH Revision No:	1.2
Service :	Legal and Privacy Services	Last Review Date :	13/02/2019
Document Owner:	Chief legal advisor	Next Review Date:	13/02/2022
Approved by:	Executive Leadership Team (ELT)	Date First Issued:	17/03/2003
Counties Manukau Health			

If you are not reading this document directly from the Document Directory this may not be the most current version.

An Explanation of “Serious Wrongdoing” (continued)

Making Disclosure

Before Making Disclosure

Usual reporting lines first

In general, Counties Manukau District Health Board employees should use their normal management reporting lines to report serious wrongdoings.

In most instances an employee will be able to achieve a satisfactory outcome by reporting the serious wrongdoing to their own manager, the General Manager of their service or hospital, or some other senior staff member.

When a disclosure may be warranted

However, there may be occasions when an employee:

- reports a serious wrongdoing through their normal management reporting lines and they believe on reasonable grounds that the outcome leaves the serious wrongdoing uncorrected or creates a further serious wrongdoing; or
- believes on reasonable grounds that if they report the serious wrongdoing through their normal management reporting lines there may be retaliatory action against them; or
- believes on reasonable grounds that their manager is involved in the serious wrongdoing or is closely associated with people involved in the serious wrongdoing.

If any of the above apply, the employee can use this internal procedure for disclosure in accordance with the Act (see below).

Internal (CMDHB) Disclosure

Address to Receiver

If a Counties Manukau DHB employee believes they have grounds for making a protected disclosure of serious wrongdoing, as previously defined, they should make that disclosure, in confidence, to:

Legal Adviser/Privacy Officer (Janet Anderson-Bidois)
Counties Manukau District Health Board Office
(Telephone : 2760044 Extn 7609)

Continued...

Document ID:	A5719	CMH Revision No:	1.2
Service :	Legal and Privacy Services	Last Review Date :	13/02/2019
Document Owner:	Chief legal advisor	Next Review Date:	13/02/2022
Approved by:	Executive Leadership Team (ELT)	Date First Issued:	17/03/2003
Counties Manukau Health			

If you are not reading this document directly from the Document Directory this may not be the most current version.

Making Disclosure (continued)

Internal (CMDHB) Disclosure (continued)

Disclosure by letter

If the employee reports the serious wrongdoing by letter, they should include details of how they can be contacted.

Unless the employee requests otherwise, they will be contacted discreetly within 5 working days to discuss how the matter should be handled.

Escalation

Where an employee believes on reasonable grounds either that the above person is or may be involved in the serious wrong-doing, or is closely associated with the people involved in the serious wrongdoing, the employee may make the disclosure to Counties Manukau District Health Board's Chief Executive Officer.

If the employee believes on reasonable grounds that the Chief Executive Officer is or may be involved in the serious wrongdoing they may report the matter to an 'appropriate authority' as outlined in "External Disclosure" (see below).

External Disclosure

Disclosure to an outside authority

An employee may be protected by the Act when making disclosure to an 'appropriate authority' outside CMDHB where they believe on reasonable grounds:

- that CMDHB's Chief Executive is or may be involved in the serious wrongdoing; or
- that immediate reference to an 'appropriate authority' is justified by the urgency of the matter or some other exceptional circumstances, or
- there has been no action or recommended action on the matter to which the disclosure relates within 20 working days of the employee having made the disclosure in accordance with CMDHB's internal procedure.

Continued...

Document ID:	A5719	CMH Revision No:	1.2
Service :	Legal and Privacy Services	Last Review Date :	13/02/2019
Document Owner:	Chief legal advisor	Next Review Date:	13/02/2022
Approved by:	Executive Leadership Team (ELT)	Date First Issued:	17/03/2003
Counties Manukau Health			

If you are not reading this document directly from the Document Directory this may not be the most current version.

Making Disclosure (continued)

External Disclosure (continued)

Appropriate authority

The employee may choose the authority or authorities most relevant to the nature of the serious wrongdoing he or she is disclosing. The Act says ‘appropriate authority’, without limiting the meaning of that term, includes:

- The Commissioner of Police
- The Controller and Auditor-General
- The Director of the Serious Fraud Office
- The Inspector-General of Intelligence & Security
- An Ombudsman
- The Parliamentary Commissioner for the Environment
- The Police Complaints Authority
- The Solicitor-General
- The State Services Commissioner
- The Health & Disability Commissioner
- the head of every public sector organisation (as defined under the State Sector Act 1988)
- a private sector body which comprises members of a particular profession or calling and which has powers to discipline its members.

Note: The Act specifically states that ‘appropriate authority’ does not include a Minister of the Crown or a Member of Parliament.

Disclosure to Minister of the Crown or Ombudsman

If an employee has made a disclosure in accordance with the above provisions and they believe on reasonable grounds that the person or appropriate authority to whom the disclosure was made has decided

- not to investigate the matter; or
- has decided to investigate the matter but has not made progress with the investigation within a reasonable time after the date on which the disclosure was made to the person or appropriate authority; or
- has investigated the matter but has not taken any action in respect of the matter nor recommended the taking of action in respect of the matter, as the case may require;

and the employee continues to believe on reasonable grounds that the information disclosed is true or likely to be true, the employee can make a disclosure to a Minister of the Crown or an Ombudsman.

Continued...

Document ID:	A5719	CMH Revision No:	1.2
Service :	Legal and Privacy Services	Last Review Date :	13/02/2019
Document Owner:	Chief legal advisor	Next Review Date:	13/02/2022
Approved by:	Executive Leadership Team (ELT)	Date First Issued:	17/03/2003
Counties Manukau Health			

If you are not reading this document directly from the Document Directory this may not be the most current version.

Making Disclosure (continued)

External Disclosure (continued)

CMDHB as an appropriate authority

In some circumstances, CMDHB may be an appropriate authority, as defined in the Act, which is able to receive protected disclosures relating to serious wrongdoing in respect of other organisations. Any disclosure of this nature that is received will be dealt with in accordance with the relevant statutory requirements.

Protection

Disclosures that are not protected

An employee is not authorised to disclose information protected by legal professional privilege.

This includes information prepared by or for lawyers for the purpose of giving or receiving legal advice. It also includes documents prepared to enable lawyers to conduct or advise on litigation.

A disclosure is not a protected disclosure if an employee makes an allegation they know to be false or they otherwise act in bad faith.

Protection provided

If an employee makes a protected disclosure of information in accordance with the information contained in this document, they will have the following protection:

1. In the unlikely event of retaliatory action by CMDHB against the employee for making or referring the disclosure, the employee may have grounds for a personal grievance action against CMDHB.
2. The employee will be immune (see "Immunity" below) from any civil or criminal proceeding or any disciplinary proceeding by reason of having made or referred that disclosure of information.

This protection overrides any enactment, rule of law, contract, oath or practice, including the Privacy Act 1993 and codes made under that Act.

Immunity

The employee may not be immune from civil or criminal or disciplinary proceedings if they were personally involved in the serious wrongdoing they disclose.

However their cooperation in reporting the wrongdoing will be taken into account in decisions on any action that may be taken against them.

Document ID:	A5719	CMH Revision No:	1.2
Service :	Legal and Privacy Services	Last Review Date :	13/02/2019
Document Owner:	Chief legal advisor	Next Review Date:	13/02/2022
Approved by:	Executive Leadership Team (ELT)	Date First Issued:	17/03/2003
Counties Manukau Health			

If you are not reading this document directly from the Document Directory this may not be the most current version.

released under Official Information Act - ref OIA 23062020 Van Wey Lovatt

Document ID:	A5719	CMH Revision No:	1.2
Service :	Legal and Privacy Services	Last Review Date :	13/02/2019
Document Owner:	Chief legal advisor	Next Review Date:	13/02/2022
Approved by:	Executive Leadership Team (ELT)	Date First Issued:	17/03/2003
Counties Manukau Health			

If you are not reading this document directly from the Document Directory this may not be the most current version.

Protection (continued)

Confidentiality

As a general rule, the identity of an employee who makes a protected disclosure must be kept confidential.

The person to whom a protected disclosure is made or referred must use his or her best endeavours not to disclose information that might identify the employee.

Exceptions

There are exceptions to the general rule of confidentiality above which are:

- a) where the employee consents in writing to the disclosure of their identity;
- b) the person who has acquired knowledge of the protected disclosure reasonably believes that disclosure of identifying information:
 - (i) is essential to the effective investigation of the allegations in the protected disclosure; or
 - (ii) is essential to prevent serious risk to public health or public safety or the environment; or
 - (iii) is essential having regard to the principles of natural justice

Grounds for refusing identification

The above confidentiality provisions can be cited by Counties Manukau DHB as grounds for refusing disclosure of information requested pursuant to the Official Information Act 1982, if that disclosure might identify a person who has made a protected disclosure.

Continued...

Document ID:	A5719	CMH Revision No:	1.2
Service :	Legal and Privacy Services	Last Review Date :	13/02/2019
Document Owner:	Chief legal advisor	Next Review Date:	13/02/2022
Approved by:	Executive Leadership Team (ELT)	Date First Issued:	17/03/2003
Counties Manukau Health			

If you are not reading this document directly from the Document Directory this may not be the most current version.

Timing

Timeline

The table below shows the time line for investigation and development of an implementation plan by the Receiver of the information (usually the Legal Adviser/Privacy Officer or the Chief Executive).

Day(s)	Action / Activity
1	Employee discloses information to the Receiver.
2	The Receiver will talk to you about the details of the serious wrongdoing.
3-14	The Receiver must carry out an investigation in accordance with the procedures set out in the policy.
15	Investigation must be completed and where appropriate the receiver will ensure the employee is aware of the investigation and outcome.
15-18	The Receiver must have completed a plan of action (following completion of the investigation) and the Receiver and persons appointed by him or her must begin implementing the plan.
20	The Receiver and persons appointed by him or her must have implemented the plan and must ensure that the recommendations made in the plan are effectively being met. Note that if the Receiver has not taken this action within 20 working days of receiving the disclosure, then you may make the disclosure to an appropriate authority.

Continued...

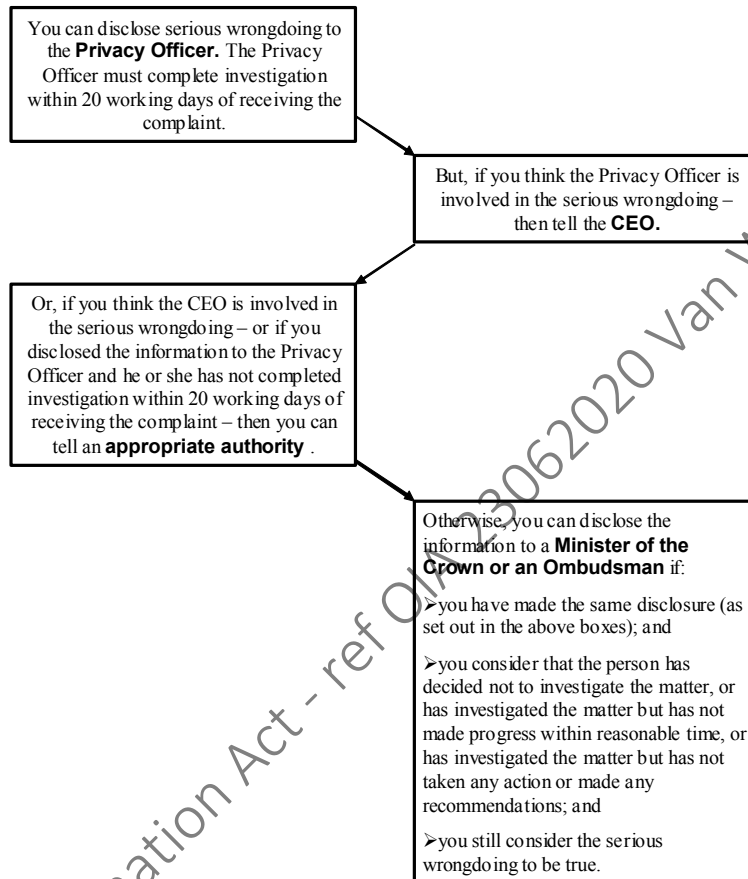
Document ID:	A5719	CMH Revision No:	1.2
Service :	Legal and Privacy Services	Last Review Date :	13/02/2019
Document Owner:	Chief legal advisor	Next Review Date:	13/02/2022
Approved by:	Executive Leadership Team (ELT)	Date First Issued:	17/03/2003
Counties Manukau Health			

If you are not reading this document directly from the Document Directory this may not be the most current version.

Deciding Who to Disclose To

Decision chart

The diagram below shows the options when deciding who to contact to receive your disclosure.



Associated Documents

Other documents relevant to this policy are listed below:

NZ Legislation	<ul style="list-style-type: none"> • Employment Relations Act 2000 • Health Information Privacy Code 1994 • Official Information Act 1982 • Privacy Act 1993 • Protected Disclosures Act 2000 • State Sector Act 1988
CMDHB Organisational Policies	<ul style="list-style-type: none"> • Discipline & Dismissal

Document ID:	A5719	CMH Revision No:	1.2
Service :	Legal and Privacy Services	Last Review Date :	13/02/2019
Document Owner:	Chief legal advisor	Next Review Date:	13/02/2022
Approved by:	Executive Leadership Team (ELT)	Date First Issued:	17/03/2003
Counties Manukau Health			

If you are not reading this document directly from the Document Directory this may not be the most current version.

Policy: Discipline & Dismissal

Policy: Discipline & Dismissal	1
Purpose	2
Scope	2
Policy	2
Authority	2
Use of disciplinary action	2
Pre-requisite	3
Adherence to process	3
Application of Discipline	3
Appropriateness & consistency	3
Procedural fairness	3
Summary dismissal	3
Grounds for Taking Disciplinary Action	4
General	4
Misconduct	4
Serious misconduct	5
Poor performance	6
Warnings	6
Sequence	6
Suspension	7
Definition	7
Purpose	7
With or without pay	7
Principles	7
Procedural Fairness	8
Timing	8
Informal preliminary meeting	8
Invitations to disciplinary meetings	8
Information	8
Witnesses	8
Meeting format	9
Requirements for Improvement	9
Maintaining written records	9
Storage & handover of written records	9
Warning period	10
Personal Grievances	10
General	10
HR involvement	10
Associated Documents	10
Definitions	11

Document ID:	A5704	CMH Revision No:	1.1
Service :	N/A - Controlled document used across the organisation	Last Review Date :	14/02/2019
Document Owner:	Director - Human Resources	Next Review Date:	14/06/2019
Approved by:	Executive Leadership Team (ELT)	Date First Issued:	19/12/2002
Counties Manukau Health			

If you are not reading this document directly from the Document Directory this may not be the most current version.

Purpose

The purpose of this policy is to provide Managers with a clear framework for managing disciplinary processes in a procedurally fair and legally correct manner.

Counties Manukau DHB treats every individual employee with fairness in regard to disciplinary matters.



Note: This policy must be read in conjunction with DISCIPLINE & DIMISSAL PROCEDURE.

Scope

This policy is applicable to all employees of Counties Manukau DHB and all Managers with authority to take disciplinary action or to dismiss staff.

Policy

Authority

The GM Human Resources and General Managers have the authority to terminate employment. General Managers should however consult the appropriate Human Resources Service Manager prior to taking any action. (Refer to the Delegated Authority Policy.)

The CMDHB Delegated Authority document details levels of authority for the issuing of disciplinary warnings.

It is possible for General Managers to sub-delegate authority for disciplinary matters to Service Managers or RC Managers where appropriate, but it is important that the Human Resources Service Manager be first advised of the existence or likelihood of disciplinary procedures being undertaken.

Use of disciplinary action

Disciplinary action may be taken in cases of:

- misconduct
- serious misconduct
- poor performance

In instances of alleged serious misconduct the disciplinary process must be implemented immediately.

If a Manager is unsure whether or not to use this policy as a result of employee behaviour, she/he should contact Human Resources.

Document ID:	A5704	CMH Revision No:	1.1
Service :	N/A - Controlled document used across the organisation	Last Review Date :	14/02/2019
Document Owner:	Director - Human Resources	Next Review Date:	14/06/2019
Approved by:	Executive Leadership Team (ELT)	Date First Issued:	19/12/2002
Counties Manukau Health			

If you are not reading this document directly from the Document Directory this may not be the most current version.

Pre-requisite

Disciplinary action should, where at all possible and appropriate, be preceded by a counselling/performance improvement session with the employee and the immediate manager (i.e. advice and / or training, guidance on work standards and expected levels of performance and conduct).

A counselling interview in itself may be advisory in nature and not necessarily followed by disciplinary action.

Adherence to process

This policy needs to be read in conjunction with the Discipline & Dismissal Process. This process must be adhered to when dealing with staff on matters of performance and alleged misconduct.

Application of Discipline

Appropriateness & consistency

Disciplinary action should match the seriousness of the incident and/or frequency of occurrence. Disciplinary action must be warranted.

It is essential that disciplinary actions are applied consistently to all employees. That is, an employee should not be treated more harshly than another in similar circumstances. Any action must also be administered fairly, and according to the rules of 'natural justice'.

Procedural fairness

When disciplining or dismissing an employee, Managers should ensure that they treat the employee fairly. (See [Procedural Fairness](#))

If Managers do not do this, the disciplinary action or dismissal may at a later date be found to be unjustified on the basis of procedural unfairness, even if there were good reasons for the action.

Summary dismissal

Sometimes, in the case of serious misconduct on the employee's part, summary dismissal may be acceptable, but even in such cases the principles of fairness must be applied.

If a Manager thinks that the behaviour of an employee may warrant summary dismissal she / he should contact the appropriate Human Resources Services Manager directly, and also discuss the matter with their immediate Manager and General Manager.

Document ID:	A5704	CMH Revision No:	1.1
Service :	N/A - Controlled document used across the organisation	Last Review Date :	14/02/2019
Document Owner:	Director - Human Resources	Next Review Date:	14/06/2019
Approved by:	Executive Leadership Team (ELT)	Date First Issued:	19/12/2002
Counties Manukau Health			

If you are not reading this document directly from the Document Directory this may not be the most current version.

Grounds for Taking Disciplinary Action

General

Disciplinary action may be taken on the grounds of:

- misconduct
- serious misconduct, or
- poor performance

Misconduct

The following constitute misconduct generally however, depending on the specific behaviour and circumstances, may also constitute serious misconduct. This list is for the purpose of illustration and is not exhaustive.

- Absenteeism without reason and notification within the time required.
- Breach of organisational policies, including but not limited to, informed consent, patients' code of rights, health and safety, privacy, human resources and service update requirements.
- Driving in a manner likely to endanger staff or cause damage to company property or vehicles;
- Being charged with a driving offence that may result in criminal conviction.
- Failing to account for absences on sick leave.
- Failing to perform duties to an acceptable standard.
- Failing to use time sheets or other prescribed time records.
- Irresponsible or unacceptable behaviour including using obscene or abusive language which could cause offence.
- Misuse of company property for purposes other than those for which it is intended.
- Posing a risk by failing to use safety equipment appropriately, or failing to abide by the safety rules and / or failing to report any accident where reporting is mandatory (this includes back strains, slipping).
- Posting unauthorised material on company notice boards.
- Reporting to work in a condition that, in the opinion of the Manager, makes the employee unable to carry out duties properly and safely.
- Smoking in any area officially designated as non-smoking, including company pool vehicles.
- The reckless or negligent introduction of computer viruses to CMDHB information systems.
- Other actions deemed by CMDHB to be similar in nature to the above.

Document ID:	A5704	CMH Revision No:	1.1
Service :	N/A - Controlled document used across the organisation	Last Review Date :	14/02/2019
Document Owner:	Director - Human Resources	Next Review Date:	14/06/2019
Approved by:	Executive Leadership Team (ELT)	Date First Issued:	19/12/2002
Counties Manukau Health			

If you are not reading this document directly from the Document Directory this may not be the most current version.

Serious misconduct

Counties Manukau DHB has rules that are required of its staff in order to provide a safe and acceptable working environment for others. The following therefore constitute matters that may be considered serious misconduct and may result in instant dismissal from Counties Manukau DHB. This list is for the purpose of illustration and is not exhaustive.

- Acceptance or solicitation of gifts or payments while representing Counties Manukau DHB, without proper authorisation.
- Assaulting or threatening another person while on Counties Manukau DHB's business.
- Harassment of a CMDHB staff member or member of the public.
- Being in possession of, taking from Counties Manukau DHB's premises, or movement of any Counties Manukau DHB property or property belonging to another employee, without proper authorisation.
- Being unsafe to practise in a health service situation, including non-presentation of a current Annual Practising Certificate.
- Breach of professional / clinical Code of Practice or Code of Ethics.
- Bringing to, or consuming on the premises (or other workplace), drugs, other than those prescribed by one's own doctor, or any intoxicating liquor without proper authority.
- Causing injury or endangering the safety of staff or the public.
- Conduct that could seriously damage the reputation of an individual or Counties Manukau DHB.
- Conviction of a criminal offence.
- Deliberately or negligently committing any act which seriously affects the quality of service or delivery of care, or results in wastage and / or damage to property.
- Failure to declare to Counties Manukau DHB, or being involved in any activities that cause, a conflict of interest with duties as an employee of Counties Manukau DHB.
- Falsifying any Counties Manukau DHB records or documentation including timesheets, or other time records, taxi, meal or other vouchers, sick leave or ACC record.
- Gambling on Counties Manukau DHB's premises without proper authorisation.
- Having an unauthorised interest, whether financial, employment or otherwise, with an organisation which does or might compete with Counties Manukau DHB or one of its subsidiaries, or which may cause a conflict of interest with the employee's duties at Counties Manukau DHB.
- Irresponsible or unauthorised use of fire prevention equipment, motor vehicles or other company property.

Document ID:	A5704	CMH Revision No:	1.1
Service :	N/A - Controlled document used across the organisation	Last Review Date :	14/02/2019
Document Owner:	Director - Human Resources	Next Review Date:	14/06/2019
Approved by:	Executive Leadership Team (ELT)	Date First Issued:	19/12/2002
Counties Manukau Health			

If you are not reading this document directly from the Document Directory this may not be the most current version.

Discipline & Dismissal

- Misuse of information obtained in the course of employment with Counties Manukau DHB.
- Refusal or failure to obey any lawful and reasonable instruction, including 'walking off the job' without authorisation, or refusal to wear required protective clothing supplied by Counties Manukau DHB.
- Sexual harassment of any person, while on Counties Manukau DHB business or premises.
- The intentional introduction or dissemination of computer viruses using Counties Manukau DHB information systems.
- The downloading, storing, dissemination and/or viewing of pornographic material using Counties Manukau DHB information systems.
- Unauthorised disclosure of information relating to Counties Manukau DHB as a business, whether to the media or otherwise.
- Other actions deemed by Counties Manukau DHB to be similar in nature to the above, including any misconduct referred to under Misconduct in this code which seriously affects the operations of Counties Manukau DHB.
- Blatant breach of The Privacy Act.

Poor performance

Poor performance can constitute grounds for taking disciplinary action where the employee has not made appropriate progress despite support and assistance.

Often, however, this can be managed through performance improvement processes that establish clear expectations of staff and identify support for staff in attaining them. This involves negotiation, agreed expectations, agreed timeframes, feedback and evaluation.

Warnings

Sequence

Generally, in disciplinary situations the sequence of warnings is:

1. verbal
2. written
3. final written

However, each case must be assessed separately, and serious misconduct may result in instant dismissal after an appropriate investigation (i.e. there may be no warnings issued)

It may be appropriate to go straight to a written warning or final written warning depending on the seriousness of the misconduct.

Document ID:	A5704	CMH Revision No:	1.1
Service :	N/A - Controlled document used across the organisation	Last Review Date :	14/02/2019
Document Owner:	Director - Human Resources	Next Review Date:	14/06/2019
Approved by:	Executive Leadership Team (ELT)	Date First Issued:	19/12/2002
Counties Manukau Health			

If you are not reading this document directly from the Document Directory this may not be the most current version.

For Warning Process refer to the Discipline & Dismissal Procedure

Suspension

Definition

Suspension is the removal of an employee from work while an allegation of a serious nature in relation to that employee is investigated, or while a decision is being made following a formal investigation meeting.

Suspension is NOT of itself a disciplinary action. It is a step to ascertain if disciplinary action is to be taken.

Purpose

Suspension may be applied if the employee's continued presence in the workplace would pose potential risk, be likely to hinder an investigation, or is such that work simply can not continue until the allegation is rebutted.

Suspension may also be used to reduce tension in the workplace and give the employee some respite from the situation.

With or without pay

Suspension will generally be on pay.

A suspension on pay is applied only by the General Manager of the relevant service, in consultation with the Human Resources Service Manager.

A suspension without pay is applied only by the GM Human Resources.

Principles

Principles which must be applied when considering implementation of a suspension are that:

- the allegation directly impinges on the employee's ability to carry out their duties (e.g. unauthorised possession of company property, serious misconduct / negligence, clinical or patient safety, violent behaviour)
- other alternatives to suspension have first been considered
- the employee is given the opportunity to put forward his/her views relating to the suspension and these are considered by the relevant manager prior to any decision being made
- the suspension does not of itself predetermine the outcome of any investigation or decision
- the suspension is necessary for a proper and fair investigation or deliberation
- the suspension does not prejudice the employee's ability to defend themselves or prepare themselves for any disciplinary action

Document ID:	A5704	CMH Revision No:	1.1
Service :	N/A - Controlled document used across the organisation	Last Review Date :	14/02/2019
Document Owner:	Director - Human Resources	Next Review Date:	14/06/2019
Approved by:	Executive Leadership Team (ELT)	Date First Issued:	19/12/2002
Counties Manukau Health			

If you are not reading this document directly from the Document Directory this may not be the most current version.

For Suspension Process refer to the Discipline & Dismissal Procedure

Procedural Fairness

Timing

When a suspected breach of disciplinary code occurs, it is important to act PROMPTLY.

Action must be taken as close as practicably possible to the time the event occurred, or comes to the attention of the delegated manager, to ensure the employee does not conclude that the behaviour is condoned. This does not mean, however, that any less time should be spent investigating the facts and ensuring procedural fairness.

Informal preliminary meeting

In order to assess the situation adequately, an informal preliminary meeting with the employee concerned may be necessary, prior to making a decision as to whether or not to proceed through the disciplinary process.

This preliminary meeting need not precipitate any disciplinary action, but may do so if there appear to be grounds for doing so. At this stage, support people may attend, and the Manager should maintain a written record of the meeting.

Invitations to disciplinary meetings

Once formal procedures have been deemed necessary, the Manager should advise the employee in advance that they wish to speak to him / her about a disciplinary matter and that they have the right to representation should they wish. This should be confirmed in writing. Sufficient warning should be given to allow the employee time to arrange for a union or other representative or support.

Information

The employee should be given full details of the allegation and should always be warned in advance that it may lead to further disciplinary action. This should be confirmed or conveyed in writing.

The employee should be given time to consider the allegations and meet with their representative to prepare their response prior to the meeting.

Witnesses

At any discipline related meeting (formal or informal):

- the Manager should have another management representative in attendance (usually their HR Service Manager)

Document ID:	A5704	CMH Revision No:	1.1
Service :	N/A - Controlled document used across the organisation	Last Review Date :	14/02/2019
Document Owner:	Director - Human Resources	Next Review Date:	14/06/2019
Approved by:	Executive Leadership Team (ELT)	Date First Issued:	19/12/2002
Counties Manukau Health			

If you are not reading this document directly from the Document Directory this may not be the most current version.

Discipline & Dismissal

- the employee should have a representative and/or support person present if they wish and should be advised of the attendance of an additional management representative.

Meeting format

At any disciplinary meeting, the

- Manager should state the alleged behaviour that is reported and seek comment from the employee first
- employee must be given the opportunity to explain their version of events

Due consideration should be given to the explanations. This might be done in an adjournment or in a follow-up interview with witnesses others as necessary. Managers must investigate the facts fully, freely, without prejudice and without haste or delay.

Requirements for Improvement

Where steps for improvement are required, the standards of necessary behaviour should be clearly stated, together with the timeframe within which they should be achieved.

Consideration should also be given to whether the individual needs assistance (eg: training) in order to improve and meet the specified standards. This should be formally arranged with the person(s) asked to provide assistance, and their report of the employee's progress should be received formally.

Maintaining written records

A written record should be kept of all discussions and warnings. The following details should be included:

- date / time of discussions
- a statement of the problem
- reference to previous current warnings
- identification of any rule violated
- corrective action required of the employee
- proposed action by the employer failing corrective action
- time in which to improvement is required (where the problem is ongoing rather than related to a single incident), up to a maximum of six months (e.g. "we will review progress monthly for three months")

Storage & handover of written records

During a disciplinary process the Manager is required to ensure that all written records are securely stored.

Document ID:	A5704	CMH Revision No:	1.1
Service :	N/A - Controlled document used across the organisation	Last Review Date :	14/02/2019
Document Owner:	Director - Human Resources	Next Review Date:	14/06/2019
Approved by:	Executive Leadership Team (ELT)	Date First Issued:	19/12/2002
Counties Manukau Health			

If you are not reading this document directly from the Document Directory this may not be the most current version.

Discipline & Dismissal

At the conclusion of a disciplinary process (to be determined between the Manager and Human Resources), originals of all documents will be managed within the guidelines of the Employee Records Policy.

Warning period

Generally warnings (verbal and written) will be for a period of up to twelve months, although there may be instances where a warning is issued for a longer period.

After the expiry of the warning period, subject to continued satisfactory performance, the warning will be lifted and no further action can be taken specifically in relation to the incident, actions or omissions that resulted in the warning.

The record of the warning will however remain permanently on the employee's personal file as part of their employment history with CMDHB.

Personal Grievances

General

All employees have a legal right to challenge a manager's decision to discipline or dismiss.

Clear, transparent and consistent processes are essential.

HR involvement

It is important that managers establish and maintain contact with Human Resources throughout the disciplinary process to confirm procedures and minimise the risk of successful personal grievances.

Associated Documents

Other documents relevant to this policy are listed below:

NZ Legislation	<ul style="list-style-type: none"> • Employment Relations Act 2000 • Professional / Clinical Codes of Practice and /or Codes of Ethics • Privacy Act 1993
CMDHB Organisational Policies	<ul style="list-style-type: none"> • Delegated Authority (Delegated Authority) • Employee Records (HR) • Exit & Termination (HR) • Occupational Health policies • Leave (HR) • Discipline & Dismissal Process

Document ID:	A5704	CMH Revision No:	1.1
Service :	N/A - Controlled document used across the organisation	Last Review Date :	14/02/2019
Document Owner:	Director - Human Resources	Next Review Date:	14/06/2019
Approved by:	Executive Leadership Team (ELT)	Date First Issued:	19/12/2002
Counties Manukau Health			

If you are not reading this document directly from the Document Directory this may not be the most current version.

Discipline & Dismissal

Other related documents	<ul style="list-style-type: none"> • Individual Employment Agreements • Collective Employment Agreements • CMDHB Code of conduct / Shared Expectations
--------------------------------	---

Definitions

Terms and abbreviations used in this document are described below:

Term/Abbreviation	Description
Misconduct	See page 4
Serious misconduct	See page 5

released under Official Information Act - ref OIA 23062020 Van Wey Lovatt

Document ID:	A5704	CMH Revision No:	1.1
Service :	N/A - Controlled document used across the organisation	Last Review Date :	14/02/2019
Document Owner:	Director - Human Resources	Next Review Date:	14/06/2019
Approved by:	Executive Leadership Team (ELT)	Date First Issued:	19/12/2002
Counties Manukau Health			

If you are not reading this document directly from the Document Directory this may not be the most current version.

Policy: CM Health Incident Reporting and Investigation

Purpose

The purpose of this policy is to outline the requirements for reporting, investigating and managing the outcomes of incidents involving consumers, workers, contractors or visitors that occur within all Counties Manukau Health (CM Health) workplaces (including buildings, grounds, vehicles and other locations where CM Health workers undertake their duties).

The primary goal of the incident reporting and management systems is to assist CM Health to effectively manage the incident reporting and investigation process including adverse events and serious harm, by ensuring incident management follows a structured process.

Objectives

1. To ensure that the appropriate process is undertaken for the investigation of all incidents, near miss and adverse events.
2. To ensure that there is immediate management of an incident when required and that every incident is appropriately prioritised, investigated and managed.
3. To ensure transparency of approach when responding to an incident that places the consumer, visitor and worker central to the response. This includes the process of open discussion and on-going communication with the consumer, visitor and worker and their support person(s).
4. To create a “just culture” where it is safe to report incidents and where a systems approach to incidents and investigation is used.
5. To identify opportunities to improve the quality and experience of care through ensuring the Incident system is a planned and co-ordinated process that links to the quality and risk management system.
6. To minimise risk and prevent future incidents through development of appropriate action plans, recommendations and review.
7. To meet statutory and/or regulatory requirements through informing workers of their responsibilities in relation to essential notification reporting and ensuring the correct authority is notified in an accurate and timely manner by the organisation.
8. Ensure integration of feedback, complaints, consumer and worker feedback, credentialed specialists and allied health personnel feedback where appropriate.



Note: This policy should be read in conjunction with the A Just Culture Policy, CMH Health and Safety Policy and the Open Disclosure with Patients Policy. For Occupational Health and Safety (OHSS) incidents refer to the CM Health Workplace Incident Reporting and Management Procedure. For rating tools and frameworks refer to Health Quality & Safety Commission’s (HQSC) Severity Assessment Code (SAC) rating and triage tool for adverse event report <https://www.hqsc.govt.nz/our-programmes/adverse-events/publications-and-resources/publication/2937/>

Document ID:	A5521	CMH Revision No:	4.0
Service :	N/A - Controlled document used across the organisation	Last Review Date :	20/02/2019
Document Owner:	Chief Medical Officer (CMO) - Executive Management	Next Review Date:	20/02/2022
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	18/03/2019
<i>If you are not reading this document directly from the Document Directory this may not be the most current version.</i>			

Scope of Use

This policy applies to any incident resulting in harm, loss or damage, to any person, property or environment, including near miss events occurring in any CM Health controlled site or location deemed to be a CM Health “Place of Work”.

This policy is applicable to:

- Any consumer or visitor within CM Health places of work.
- All CM Health workers (full-time, part-time, casual and temporary), and associated personnel (including contractors, students, visiting health professional etc.) working in, or contracted to provide a service on any CM Health site.
- Any person undertaking work activity on a CM Health controlled site, e.g. sales representative, stall holder.

Policy

Incident Reporting

All CM Health workers described within the scope above or their representative (where applicable) have a professional, moral and, where physical injury is involved, legal responsibility to report any incident. This includes clinical, corporate and environmental incidents involving or affecting (or where there is potential to affect) consumers, visitors, workers and contractors.

1. Incidents should be reported promptly and accurately as soon as practicable, preferably on the same working day.
2. The primary mode of reporting consumer, workers and visitor incidents is through the electronic organisational incident reporting system (IRS).
3. There is also a responsibility to notify relevant managers and/or senior clinical workers where appropriate.

Notifiable Events

Where a Notifiable Event has occurred, there are legal and contractual responsibilities to report incidents to external parties. A Notifiable event includes a Notifiable Injury or Incident (see definitions). Any notifiable event must be reported immediately to the OHSS or Duty Manager (after hours). CM Health will endeavour to report all such events to the respective regulatory body in accordance with legislative requirements.

Incidents involving consumers

All consumer incidents resulting in serious injury or death (includes notifiable injury) as a result of clinical care processes or non-clinical care processes (All SAC 1 & 2 scores) are to be notified to the Adverse Event Operational Group.

Any consumer incidents (all SAC codes) involving non-clinical causes* are also to be reported to OHSS for further follow up to ensure all involved hazards are identified and mitigated.

* Incidents involving consumers may involve **non-clinical causes** (for example: slipping on a wet floor, faulty equipment, unsafe environment). This is in contrast to incidents that occur due to a **clinical care process** (for example: medication error, wrong site surgery, delayed diagnosis).

Document ID:	A5521	CMH Revision No:	4.0
Service :	N/A - Controlled document used across the organisation	Last Review Date :	20/02/2019
Document Owner:	Chief Medical Officer (CMO) - Executive Management	Next Review Date:	20/02/2022
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	18/03/2019
If you are not reading this document directly from the Document Directory this may not be the most current version.			

Incident Investigation

A 'systems approach' is to be used in the investigation of all incidents; this involves determining what went wrong with the systems of work, systems of care and/or services, why the incident occurred and what corrective action is needed to mitigate the risk of recurrence. It is not intended to identify who was at fault or to assign blame.

Investigation of incidents involving consumers:

Consumer incidents occurring as a result of clinical processes of care are managed at the appropriate organisational, service management and clinical levels as per the appropriate consumer incident investigation procedure.

Where harm involving a consumer has occurred as a result of a non-clinical process, OHSS will also be involved in the investigation process and may lead the investigation where appropriate in accordance with OHSS Incident investigation procedure.

Significant incidents involving consumers subject to the Mental Health Act may also be investigated through the Mental Health Service Serious Incident Review Panel (SIRP) and information provided to the Adverse Event Operational Group as per departmental procedures.

Investigation of incidents involving workers:

Worker incidents are investigated and followed up to resolution by the worker's manager with support from the OHSS. All workplace hazards/risks identified by the investigation are to be mitigated in accordance with CM Health procedures and recorded in the Department/Service Hazard/Risk Register.

Any OHSS investigation will involve the manager, affected workers and a health and safety representative, as appropriate and all information regarding the findings and corrective actions required will be recorded on the electronic Incident Reporting System (IRS). Notifiable Injuries or Incidents may also be recorded on the OHS Notifiable Event Investigation Form.

Non notifiable incidents will be investigated by the appropriate manager and the findings, corrective action and feedback to workers will be recorded on the incident report. OSHH will review the findings and corrective action.

Investigation of incidents involving visitors and contractors:

Incidents involving all visitors are followed up to resolution by the appropriate department manager with support from the OHSS and/or the contracts manager where the incident involves a contractor.

Where incidents have occurred involving contractors, the contractor and contractor's employer will also be responsible for investigating and following up the incident, this will include providing notification to CM Health and is to be recorded in the IRS. (Refer CM Health's Health and Safety Manual).

Document ID:	A5521	CMH Revision No:	4.0
Service :	N/A - Controlled document used across the organisation	Last Review Date :	20/02/2019
Document Owner:	Chief Medical Officer (CMO) - Executive Management	Next Review Date:	20/02/2022
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	18/03/2019

If you are not reading this document directly from the Document Directory this may not be the most current version.

released under Official Information Act - ref OIA 23062020 Van Wey Lovatt

Document ID:	A5521	CMH Revision No:	4.0
Service :	N/A - Controlled document used across the organisation	Last Review Date :	20/02/2019
Document Owner:	Chief Medical Officer (CMO) - Executive Management	Next Review Date:	20/02/2022
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	18/03/2019
<i>If you are not reading this document directly from the Document Directory this may not be the most current version.</i>			

Responsibilities

Managers are responsible to ensure workers report incidents via the appropriate process and to ensure investigations are completed in accordance with this policy and the appropriate CM Health Incident reporting and Investigation procedure.

Workers are responsible for reporting any incident or near miss incident that occurred to themselves or any service consumer in their care in accordance with CM Health Policy and procedures. Workers are expected to participate as required in any incident investigation that involves them or consumers in their care.

Definitions/Description

Terms and abbreviations used in this document are described below:

Adverse Event

Is an event with negative or unfavourable reactions or results that are unintended, unexpected or unplanned (also referred to as incident or reportable event). An event which results in unanticipated death or loss of function not related to the natural course of a consumer's illness or condition.

Always Report & Review Events

The Always Report and Review list is a subset of adverse events that should be reported and managed in the same in the same way as SAC 1 and 2-rated events, irrespective of whether or not there was harm to the consumer. Always Report and Review events are events that can result in serious harm or death but are preventable with strong clinical and organisational systems. Reporting Always Report and Review events can highlight weaknesses in how an organisation manages fundamental safety processes. The list is updated regularly by the HQSC and CMH (<https://www.hqsc.govt.nz/our-programmes/adverse-events/publications-and-resources/publication/2937/>)

Consumer

A person who uses / receives care / treatment/ services from CM Health

Contributing factor

A circumstance, action or influence which has contributed to an incident or near miss.

Harm

Is illness and/or injury, physical and/or mental harm.

Hazard

Anything with the potential to cause harm or loss to person, property or environment.

Incident

Any event that could have (near miss) or has resulted in harm, damage or loss, to any person, property or place (including environment).

Incident Management

A systematic process for identifying, notifying, prioritising, investigating and managing the outcomes of an incident and acting to prevent recurrence.

Just Culture

Staff should feel safe and supported when reporting incidents of patient harm in the knowledge that investigations seek to identify system issues and not apportion individual blame.

Near miss / close call

An event that could have resulted in harm or loss but did not.

Notifiable event

Any events that arise from work that results in the death of a person, a notifiable injury/illness or a notifiable incident.

Document ID:	A5521	CMH Revision No:	4.0
Service :	N/A - Controlled document used across the organisation	Last Review Date :	20/02/2019
Document Owner:	Chief Medical Officer (CMO) - Executive Management	Next Review Date:	20/02/2022
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	18/03/2019

If you are not reading this document directly from the Document Directory this may not be the most current version.

Risk	The possibility (likelihood) of suffering harm or loss from a hazard.
Serious Incident Review Panel (SIRP)	Is a process followed by Mental Health to review serious incidents involving consumers under the Mental Health Act.
Severity Assessment Code (SAC)	Is a numerical rating which defines the severity of an adverse event and as a consequence the required level of reporting and review to be undertaken for the event.
System failure	A fault, breakdown or dysfunction within process(es) or infrastructure.
Worker	Any person who carries out work in any capacity for CM Health (full-time, part-time, casual and temporary), including associated personnel (contractors, students, visiting health professional etc.) working in, or contracted to provide a service on any CM Health site.
Workplace	Is any place where work is carried out for or on behalf of CM Health whilst a person is deemed at work.

Associated Documents

Other documents relevant to this policy are listed below:

NZ Legislation /Standards	Health and Safety at Work Act 2015 Health and Disability Services (Safety) Act 2001 Compulsory Assessment and Treatment (Mental Health) Act 1992
CM Health Documents	Policy: A Just Culture Policy: Health and Safety Policy: Open Disclosure with Patients Policy: Serious Incident Review Panel (SIRP) Mental Health Services Policy: Consumer related Complaint and Feedback Management Policy: Code of Conduct
Other related documents	Health and Disability Sector Standards (2008) Workplace Incident Management Procedure Consumer Related Complaints and Feedback Management Procedure: Reporting and Managing Blood Body Fluid Exposure Procedure CM Health's Health and Safety Manual

Document ID:	A5521	CMH Revision No:	4.0
Service :	N/A - Controlled document used across the organisation	Last Review Date :	20/02/2019
Document Owner:	Chief Medical Officer (CMO) - Executive Management	Next Review Date:	20/02/2022
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	18/03/2019

If you are not reading this document directly from the Document Directory this may not be the most current version.

Procedure: Patient Related Incident Reporting and Management

Purpose.....2

Objectives2

 Open Disclosure 2

 Just Culture..... 2

Scope of Use.....2

Roles and Responsibilities.....3

 Frontline staff 3

 Clinical Nurse Director/Clinical Director Allied Health/ Professional Leads/CNM/Team Leader/Coordinators 3

 Clinical Quality and Risk Managers 3

 Feedback Central Role..... 3

 Adverse Events Operational Group role..... 3

 Adverse Events Governance Group..... 3

 Clinical Director/ General Manager 3

Resources.....4

Procedure.....4

 Step 4

 Incident Identification Action 4

 Person(s) responsible where relevant..... 4

 Step 5

 Immediate Action..... 5

 Person(s) responsible where relevant..... 5

 Step 6

 Notification/Reporting Action 6

 Person(s) responsible where relevant..... 6

 Step 6

 Prioritisation of Incidents..... 6

 Person(s) responsible where relevant..... 6

 Step 7

 Responding to Incidents that Occur within the Mental Health Service’..... 7

 Person(s) responsible where relevant..... 7

 Step 7

 SAC 1 and 2 Incident Management..... 7

 Person(s) responsible where relevant..... 7

 Step 8

 SAC 3 Incident Management 8

 Step 9

 SAC 4- 5 Incident Management 9

10Document ID:	A1136626	CMH Revision No:	1.0
Service:	CMDHB Governance	Last Review Date :	10/06/2020
Document Owner:	Chief Medical Officer (CMO) - Executive Management	Next Review Date:	10/06/2022
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	10/07/2019
If you are not reading this document directly from the Document Directory this may not be the most current version			

Step 9

Staff support 9

Medico-legal involvement 9

Recommendations10

Staff related Feedback and Learning.....10

Patient/responsible person (family whaanau member or other person) Feedback and Learning10

Information storage/ filing11

References 11

Definitions/Description.....11

Associated Documents..... 13

Adverse Event Checklist.....14

Feedback Central Adverse Events Process.....16

Appendix 118

Appendix 2 SAC rating and assessment21



Note: This procedure must be read in conjunction with the [Incident Reporting and Investigation Policy](#)

Purpose

The purpose of this procedure is to identify the expectations and practices associated with the identification of, reporting, investigation and response to all incidents occurring at CM Health.

Objectives

Open Disclosure

When a patient is harmed while receiving clinical treatment, it is important that the health practitioner/team respond in a manner that meets the patient’s needs and fulfils the professional, ethical and legal responsibilities of health practitioners.

It is expected that the senior clinician responsible for the care of the patient will disclose the situation that has arisen in an open, honest and accountable manner. The disclosure is to be documented. For further information, [‘The Open Disclosure Policy’](#) is available on Document Directory

Just Culture

A fair and just culture means applying a systems approach to the investigation of patient harm. This approach recognises that all individuals are error prone and that the optimum way to improve patient safety and learn from adverse events, is through staff feeling safe to voice their concerns, report errors and to investigate the underlying causes of such errors. A Just Culture policy means fair-minded treatment, having productive conversations, and creating effective structures that encourage people to reveal their errors and help the organisation learn from them.

For further information, [‘The Just Culture Policy’](#) is available on Document Directory

Scope of Use

10Document ID:	A1136626	CMH Revision No:	1.0
Service:	CMDHB Governance	Last Review Date :	10/06/2020
Document Owner:	Chief Medical Officer (CMO) - Executive Management	Next Review Date:	10/06/2022
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	10/07/2019

If you are not reading this document directly from the Document Directory this may not be the most current version

This procedure is applicable to all CM Health employees, (full-time, part-time and casual (temporary) including contractors, visiting health professionals and students working in any CM Health facility.

Roles and Responsibilities

Frontline staff

- It is the responsibility of all staff, described within the Policy Scope, to report all incidents they identify.
- Where there are multiple staff involved, only one incident log is made reflecting the experience of all involved.

Clinical Nurse Director/Clinical Director Allied Health/ Professional Leads/CNM/Team Leader/Coordinators

- Participate in SAC 1 or 2 investigations as required.
- Where advisory only, provide, where necessary input into the investigation process
- Where responsible for the monitoring and management of incidents complete follow up activities for SAC 3, 4 and 5 reported incidents. Identify cause, resolution and follow up actions. Close the incident.
- For SAC 1 and 2 incidents, participate in the organisational investigation process under the lead of the CQRM. Respond/implement action from investigations as required

Clinical Quality and Risk Managers

- Ensure (leading where appropriate) that investigations/Root Cause Analysis (RCA's) are timely, unbiased and meet best practice standards and CM Health values.
- Build staff capability in complaint and incident/adverse event investigation and management, including training for Root Cause Analysis (RCA), London Protocol (Mental Health cases) or equivalent systematic method of review
- Comply with the requirements of the Feedback Central Adverse Events Process
- Monitor the trends in incidents relevant to the area of responsibility

Feedback Central Role

- Monitor/support the practices associated in the Feedback Central Adverse Events Process

Adverse Events Operational Group role

- As in Appendix 1 receive new cases, reports for approval and provide a forum where Adverse Events are analysed and responses reviewed.
Where necessary elevate events and issues to the Adverse Event Governance Group.

Adverse Events Governance Group

- Receives reports/issues from the AEOG escalating issues that require an organisational response.

Clinical Director/ General Manager

- The General Manager/Clinical Director/Midwifery Director is responsible for the successful management and resolution of all incidents occurring within their area even if the responsibility has been delegated.
- They are responsible for:
 - The incident management and resolution process within their services ensuring appropriate involvement of patients and family.

10Document ID:	A1136626	CMH Revision No:	1.0
Service:	CMDHB Governance	Last Review Date :	10/06/2020
Document Owner:	Chief Medical Officer (CMO) - Executive Management	Next Review Date:	10/06/2022
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	10/07/2019
If you are not reading this document directly from the Document Directory this may not be the most current version			

- Detailed investigation at a service level including staff interviews may be delegated to the Service Manager, Clinical Nurse Director, Midwifery Director, Clinical Director Allied Health or other professional leader
- Managing involvement of external clinical advisers if required.
- Ensuring that the incident is escalated to the Risk Register as appropriate
- Managing Treatment Injury Claims notified by Accident Compensation and Rehabilitation Corporation (ACC) as delegated by the CMO
- Ensuring information is only released to appropriate people, taking into account relevant legislation, and ensuring that appropriate members of the Executive Leadership Team are informed.
- The Clinical Chiefs have an audit/monitoring/advisory function to ensure timelines are adhered to and to assist with clinical content of reports.

Resources

[Adverse Event Checklist](#)

[Feedback Central Adverse Events Process](#)

[Process map see Appendix 1](#)

[SAC Rating and assessment tools](#)

Procedure



Incident identification with immediate action and reporting

Incident reporting is not for staff to report on the behaviour of other staff.

Step	Incident Identification Action	Person(s) responsible where relevant
1.	An incident/accident is an unplanned clinical or non-clinical event that results in, or has the potential to result in, injury, damage or loss: <ul style="list-style-type: none"> ● Clinical: an event unrelated to the natural course of the illness and differs from the expected outcome of patient management ● Product Fault: an event where a consumable product or medical device has failed in its intended purpose ● Health and Safety: An event relating to a hazard, work injury or serious harm, involving employees, contractors, sub-contractors, students and volunteers. 	All staff
2.	An incident may be minor SAC 4-5 (e.g. medication error with no harm, piece of equipment goes missing, loss/unavailability of clinical record), moderate SAC 3 (e.g. additional monitoring, investigations or interventions as a result of incident, patient reacts to medication which should have been withheld) or serious/major SAC 1-2 (e.g. resulting in death or major serious harm).	

10Document ID:	A1136626	CMH Revision No:	1.0
Service:	CMDHB Governance	Last Review Date :	10/06/2020
Document Owner:	Chief Medical Officer (CMO) - Executive Management	Next Review Date:	10/06/2022
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	10/07/2019
If you are not reading this document directly from the Document Directory this may not be the most current version			

3.	Line managers are responsible for ensuring that staff understand what constitutes a patient “incident” and how it differs from a complication of care (an established consequence of an intervention e.g. post-operative surgical site infection).	Line managers
4.	<p>The first step in managing incidents is recognising and identifying them. Incidents may be identified by/from:</p> <ul style="list-style-type: none"> • direct observation or facilitated discussion • clinical staff or patient during or following patient care • patients or family/whaanau member expressing concerns or complaints to a staff member • the Clinical Quality and Risk Manager(s)/Coordinators • ACC reports • HDC reports • Coroner’s report • clinical record audits • morbidity/mortality reviews <p>Incident reporting system is not for situations associated with external agencies.</p>	
5.	Report incidents identified within a complaint in the Incident Reporting system.	



Note: Incident resulting in, or linked to a complaint, must be investigated and managed in the first instance as an incident, but also responded to as per the Consumer Complaints Management Policy (see associated Auckland DHB guidelines) [Consumer Related Complaints and Feedback Policy](#).

Step	Immediate Action	Person(s) responsible where relevant
1.	<p>Take immediate action to mitigate the harmful consequences of the incident.</p> <p>Such action would potentially include support for the person involved, their family and/or the staff involved in the incident.</p> <p>Take immediate action to make the local environment safe e.g. the removal of a hazardous substance. Call for assistance/advice as necessary.</p> <p>On discovering an event, initiate preventive or corrective action immediately to ensure person(s) safety and wellbeing. This may include:</p> <ul style="list-style-type: none"> • Additional medical treatment • Placing the patient in a safe environment • Replacing faulty equipment 	All Staff and Line Managers

10Document ID:	A1136626	CMH Revision No:	1.0
Service:	CMDHB Governance	Last Review Date :	10/06/2020
Document Owner:	Chief Medical Officer (CMO) - Executive Management	Next Review Date:	10/06/2022
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	10/07/2019
If you are not reading this document directly from the Document Directory this may not be the most current version			

	<ul style="list-style-type: none"> • Withdrawal of a service in the interests of patient safety 	
2.	In the event of serious harm to a staff member, where possible the scene of the incident should be secured by the person in charge of the workplace and notified accordingly according to the CM Health and Safety Te Haumarū Oranga Policy	Line managers
3.	For all incidents resulting in harm or possible harm to a patient, the information about the event must be given to the person involved and/or carer as soon as it is practicably possible (at least within 24 hours of the event becoming known) in an open and honest manner. Called 'Open disclosure' refer to Open Disclosure with Patients - Policy for further details.	Line Managers
4.	In some situations, it is also appropriate to secure items such as the patient's clinical record or the equipment used as it may be required for the review of the event.	Line managers or CQRM

Step	Notification/Reporting Action	Person(s) responsible where relevant
1.	Any employee of CM Health who identifies an incident can and should notify it by completing the report in the Incident Reporting system . The staff member involved in the incident completes the incident report, but any staff member who becomes aware of the incident may also complete the reporting.	All staff
2.	Complete reporting as soon as possible, preferably before the end of the working day/shift but no longer than 24 hours. Notifications must be stated in an objective, factual and professional manner. Avoid opinion and subjective comments. Identification of staff involved by name should be avoided. If unsure, seek advice from the relevant Clinical Quality and Risk Manager.	
3.	Notify other internal/external agencies as required: <ul style="list-style-type: none"> • Procurement (Materials Management) • Medsafe • HealthAlliance • Occupational Health • Medication Safety Service • For SAC 1 events in addition to notification via the automated reporting system also notify the Clinical Chiefs and or other ELT members as necessary. 	CQRM or delegated other

Step	Prioritisation of Incidents	Person(s) responsible where relevant
1.	The person reporting the incident must make an initial assessment of the severity of the incident according to the	All staff

10Document ID:	A1136626	CMH Revision No:	1.0
Service:	CMDHB Governance	Last Review Date :	10/06/2020
Document Owner:	Chief Medical Officer (CMO) - Executive Management	Next Review Date:	10/06/2022
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	10/07/2019
If you are not reading this document directly from the Document Directory this may not be the most current version			

	Health Quality Safety Commission (HQSC) SAC rating system (see SAC Rating and assessment tools)	
2.	The rating is determined by assessing the actual outcome or consequence of the incident as known at the time of notification.	
3.	<p>If an incident is complex and the manager reviewing the incident is unclear what SAC should be assigned or the type of investigation, they must escalate the case as follows:</p> <ul style="list-style-type: none"> Ascribe the highest relevant rating until clarified as to appropriate level e.g. if not sure if a '2' or '3' log as a '2' The relevant Clinical Quality and Risk Manager / Coordinator If there is still a discrepancy or no clear SAC rating, the Clinical Quality and Risk Manager/Coordinator will present the case in the next Adverse Events Operational Group meeting, asking for advice. <p>Cases requiring escalation will be documented on the 'New Cases' list in the Adverse Events Operational Group (AEOG) folder.</p> <p>The final SAC rating must assigned on the closure of the incident, which for those rated 3-5 this is to be within 20 working days and for 1-2 rated incidents within 70 working days.</p>	Line manager CQRM
4.	Some events require mandatory external notification regardless of their risk rating. For specified incidents requiring mandatory external notification, see here .	CQRM

Step	Responding to Incidents that Occur within the Mental Health Service'	Person(s) responsible where relevant
1.	The Mental Health and Addictions Services has adapted the CM Health adverse event/serious incident review process and severity assessment code (SAC) to better support response and learning within mental health services. All reportable events go to an Adverse Event Committee that has been specifically convened for Mental Health and Addictions Services. Events are initially triaged to determine the type of review required, preliminary SAC rating, and review team. The review team typically includes representatives of those disciplines involved and a staff member to lead outreach to the family/whaanau. Once the final draft report outlining findings from the review is complete, the report goes back to the Adverse Event Committee for sign off.	

Step	SAC 1 and 2 Incident Management	Person(s) responsible where relevant
1.	Refer to Feedback Central Adverse Events Process and Appendix	

10Document ID:	A1136626	CMH Revision No:	1.0
Service:	CMDHB Governance	Last Review Date :	10/06/2020
Document Owner:	Chief Medical Officer (CMO) - Executive Management	Next Review Date:	10/06/2022
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	10/07/2019
If you are not reading this document directly from the Document Directory this may not be the most current version			

	1 for process map	
2.	STEP 1: Report event to HQSC CQRM completes Adverse Event Brief: Part A and sends to HQSC within 15 working days of notification of event to provider	CQRM
3.	All SAC 1 and SAC 2 events investigation use a detailed investigation in the form of a systemic review, such as a Root Cause Analysis (RCA), London Protocol (Mental Health cases) or equivalent systematic method of review. On completion of the investigation report the service signs off on the methods, findings and recommendations The investigation report is sent within 50 working days of the incident notification, to the AEOG for approval of findings and recommendations. On acceptance of the investigation report methods, findings and recommendation(s) an Adverse Events Brief (AEB) Part B is sent to HQSC within 70 working days of the original notification of event to provider.	CQRM
4.	An individual with relevant training and/or support is to lead the review. Members of AEOG can advise on process and methods. Investigation team members are selected by the directorate for their expertise in the subject matter relating to the event. Divisions should consider including staff members outside the immediate clinical area, where appropriate, such as other clinical services, cultural advisors, facilities management, pharmacy, allied health and materials management. Staff members directly involved in the event (or their manager) must not be included in the review team. Directorate leaders must ensure team members are released from their usual work to undertake the review. CQRM will regularly report to the lead Director about the progress towards completion of reviews.	
	A summary of the events and recommendations will be sent as AEB part B to HQSC within 70 working days of notification of event to provider.	CQRM

Step	SAC 3 Incident Management
1.	Refer to Appendix 1 for process map. These incident reviews are undertaken at the ward or service level and responsibility for their management must be assigned. Review of these incidents must identify: <ul style="list-style-type: none"> • System issues that need to be addressed • Appropriate quality improvement action to prevent recurrence where possible
2.	Potentially relevant tools include barrier analysis, cause and effect diagrams, five whys, flow diagrams and change analysis. It will not be possible to formally investigate all SAC 3 and SAC 4 events. It may be more efficient and just as appropriate to investigate multiple incidents as common incident types and to develop a common action plan.

10Document ID:	A1136626	CMH Revision No:	1.0
Service:	CMDHB Governance	Last Review Date :	10/06/2020
Document Owner:	Chief Medical Officer (CMO) - Executive Management	Next Review Date:	10/06/2022
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	10/07/2019
If you are not reading this document directly from the Document Directory this may not be the most current version			

3.	The review, or decision to aggregate events, should be completed within 30 working days and documented in the 'outcome details' section on the electronic reporting database.
----	---

Step	SAC 4- 5 Incident Management
4.	<p>Refer to Appendix 1 for process map.</p> <p>These incident reviews are undertaken at the ward or service level by the Charge Nurse manager, Team Leader or Manager.</p> <p>Review of these incidents must identify:</p> <ul style="list-style-type: none"> • System issues that need to be addressed • Appropriate quality improvement action to prevent recurrence where possible • Discuss at relevant meetings where there are concerns or opportunities to share learning's

Step	Staff support
1.	Ensure staff safety and support. Approaches might include defusing, debriefing and involving professional bodies.
2.	The Employee Assistance Programme (EAP) is available to staff members for support and debriefing.
3.	Maori staff may wish to access cultural support internally or from within their own whaanau. For internal support and advice, contact the Maori Health Team at CM Health.



Note: Protected quality assurance activity (PQAA)

CM Health's primary investigation into an adverse incident, such as an RCA, is not a PQAA activity. Staff members are to be informed about the use of information provided for any review they are asked to be involved in. Staff members may be requested to write additional information as part of the review process. Notes can be taken as review teams gather more information about an event.

Step	Medico-legal involvement
1.	Where an event has resulted in a review by the Coroner, the RCA or equivalent review may be submitted to the Coroner before the inquest. Consult with the CMH DHB Legal Counsel.
2.	For any event that may have medico-legal implications, (i.e. there is a significant adverse outcome for the patient/client and criticism of clinicians is likely) documentation other than a factual account in the clinical record and the standard notifications should be made only with legal/professional advice.
3.	Medical defence organisations and/or professional indemnity insurers require notification of potential claims. This is the responsibility of the individual professional involved.
4.	Advice can also be sought from CM Health Legal Counsel. Legal advice must not delay submission of the event via Incident Management System.

10Document ID:	A1136626	CMH Revision No:	1.0
Service:	CMDHB Governance	Last Review Date :	10/06/2020
Document Owner:	Chief Medical Officer (CMO) - Executive Management	Next Review Date:	10/06/2022
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	10/07/2019
If you are not reading this document directly from the Document Directory this may not be the most current version			

Step	Recommendations
1.	<p>Implementations of recommendations from the reviews are required to develop better systems to ensure improved practice. Recommendations should be written with the following consideration:</p> <p>Strong</p> <ul style="list-style-type: none"> • Simplify the process and remove unnecessary steps • Standardise equipment or process of care maps • Architectural/physical plant changes <p>Intermediate</p> <ul style="list-style-type: none"> • Increase staffing/decrease workload • Checklist /cognitive aid • Enhanced documentation/communication <p>Weaker</p> <ul style="list-style-type: none"> • Double checks • Warning and labels • New policy/procedure/training <p>The AEOG will review the reports from SAC 1 and SAC 2 investigations and decide whether they should be accepted in conjunction with the directorate. The directorate will consider the allocation of appropriate resources to implement the agreed recommendations.</p> <p>The acceptance of the recommendations is recorded in the minutes of the Adverse Events Operational Group meetings.</p>
2.	<p>Recommendations from SAC 1 and SAC 2 reviews must include timeframes for completion and must have an assigned person(s) responsible for the implementation of recommendations. The recommendations are added to the CMH wide corrective action database for tracking of implementation.</p>

Step	Staff related Feedback and Learning
1.	<p>Feedback must be provided to relevant staff members on the results/outcomes of investigations for all events. This must occur in a timely manner.</p> <p>For a SAC 1 event, the feedback must be provided and undertaken by senior staff and be based on the final investigation report.</p> <p>The draft report must be provided to the relevant clinical team and feedback presented at relevant staff meetings. Recommendations are to be agreed to by the service prior to being submitted to the AEOG.</p>
2.	<p>Directorates should provide ward staff members/clinical and management teams regular reports on aggregated data and outcomes of reviews. Feedback should include the changes made and the improvements achieved as a result of these changes.</p>

Step	Patient/responsible person (family whaanau member or other person)
------	---

10Document ID:	A1136626	CMH Revision No:	1.0
Service:	CMDHB Governance	Last Review Date :	10/06/2020
Document Owner:	Chief Medical Officer (CMO) - Executive Management	Next Review Date:	10/06/2022
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	10/07/2019
<p>If you are not reading this document directly from the Document Directory this may not be the most current version</p>			

Feedback and Learning	
1.	<p>Patients or whaanau members must be provided with an opportunity to discuss the outcome of the investigation unless there are exceptional reasons for not doing so. The decision to not meet/follow-up with the patient/whaanau is to be the exception not the rule.</p> <p>The meeting should be face to face if possible and may include the provision of the report and other summary material. Provide the patient/whaanau with an opportunity to meet again to discuss any questions they may have resulting from the outcome meeting or reading the report.</p>
2.	<p>Feedback should usually be made to the individual patient and/or responsible person (family/whaanau member or other person). This must occur formally for SAC 1 and 2 events. When discussion with the consumer is not possible or appropriate - such as when they have died or been significantly compromised - his or her next of kin, designated contact person, or representative must be informed.</p>
3.	<p>Cultural support and processes and/or emotional support must be considered when arranging the feedback meeting for patients or families. Details about the incident and any harm experienced and any other subsequent clinical actions must be fully documented in the patient's clinical record.</p>
4.	<p>If not previously, notified consumers must be advised at this point that they may be entitled to compensation through the ACC Treatment Injury claims process. Appropriate medical forms (ACC45 & ACC2152 - see Forms) must be initiated.</p>
5.	<p>Directorate leaders must be involved in decisions on who provides feedback to patients and their families and on when and what information is to be provided (or not). Details of staff members involved in the event must not be included in any feedback.</p>

Step	Information storage/ filing
1.	All information related to incidents is stored electronically in the Incident Management System

References

Nil.

Definitions/Description

Terms and abbreviations used in this document are described below:

Term/Abbreviation	Description
Adverse Event	Is an event with negative or unfavourable reactions or results that are unintended, unexpected or unplanned (also referred to as incident or reportable event). An event, which results in in unanticipated death or loss of function, not related to the natural course of a consumer's illness or condition.

10Document ID:	A1136626	CMH Revision No:	1.0
Service:	CMDHB Governance	Last Review Date :	10/06/2020
Document Owner:	Chief Medical Officer (CMO) - Executive Management	Next Review Date:	10/06/2022
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	10/07/2019
If you are not reading this document directly from the Document Directory this may not be the most current version			

Always Report & Review Events	The Always Report and Review list is a subset of adverse events that should be reported and managed in the same in the same way as SAC 1 and 2 rated events, irrespective of whether or not there was harm to the consumer. Always Report and Review events are events that can result in serious harm or death but are preventable with strong clinical and organisational systems. Reporting Always Report and Review events can highlight weaknesses in how an organisation manages fundamental safety processes. The list is updated regularly by the HQSC and CMH (https://www.hqsc.govt.nz/assets/Reportable-Events/Publications/National_Adverse_Events_Policy_2017/Always-report-and-review-list-2018-19-Final.pdf)
AEOG	Adverse Events Operational Group
Consumer	A person who uses / receives care / treatment/ services from CM Health
Contributing factor	A circumstance, action or influence which has contributed to an incident or near miss.
CQRM	Clinical Quality and Risk Manager
Harm	Is illness and/or injury, physical and/or mental harm.
Hazard	Anything with the potential to cause harm or loss to person, property or environment.
HQSC	Health Quality Safety Commission
Incident	Any event that could have (near miss) or has resulted in harm, damage or loss, to any person, property or place (including environment).
Incident Management	A systematic process for identifying, notifying, prioritising, investigating and managing the outcomes of an incident and acting to prevent recurrence.
Just Culture	Staff should feel safe and supported when reporting incidents of patient harm in the knowledge that investigations seek to identify system issues and not apportion individual blame.
Near miss / close call	An event that could have resulted in harm or loss but did not.
Notifiable event	Any events that arise from work that results in the death of a person, a notifiable injury/illness or a notifiable incident.
Risk	The possibility (likelihood) of suffering harm or loss from a hazard.
Serious Incident Review Panel (SIRP)	Is a process followed by Mental Health to review serious incidents involving consumers under the Mental Health Act.
Severity Assessment Code (SAC)	Is a numerical rating, which defines the severity of an adverse event and as a consequence the required level of reporting and review to be undertaken for the event.
System failure	A fault, breakdown or dysfunction within process/es or infrastructure.
Worker	Any person who carries out work in any capacity for CM Health (full- time, part-time, casual and temporary), including associated personnel (contractors, students, visiting health professional etc.) working in, or contracted to provide a service on any CM Health site.

10Document ID:	A1136626	CMH Revision No:	1.0
Service:	CMDHB Governance	Last Review Date :	10/06/2020
Document Owner:	Chief Medical Officer (CMO) - Executive Management	Next Review Date:	10/06/2022
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	10/07/2019
If you are not reading this document directly from the Document Directory this may not be the most current version			

Workplace	Is any place where work is carried out for or on behalf of CM Health whilst a person is deemed at work.
-----------	---

Associated Documents

Other documents relevant to this procedure are listed below:

NZ Legislation / Standards	Health and Safety at Work Act 2015 Health and Disability Services (Safety) Act 2001 Compulsory Assessment and Treatment (Mental Health) Act 1992 Privacy Act
CM Health Documents	Consumer Related Complaints and Feedback Policy Complaints Resolution and Management and Patient Feedback Procedure Incident Reporting and Investigation - Policy Open Disclosure with Patients - Policy A Just Culture - Policy CM Health and Safety Te Haumaru Oranga Policy Code of Conduct - Policy Media - Policy
Other related documents	Health and Disability Sector Standards (2008) Workplace Incident Management Procedure Consumer Related Complaints and Feedback Management Procedure: Reporting and Managing Blood Body Fluid Exposure Procedure CM Health’s Health and Safety Manual ADHB Incident Management - Guideline

released under Official Information Act 2000 / OIA 2000 / 2019/0152020 Van Wey Lovatt

10Document ID:	A1136626	CMH Revision No:	1.0
Service:	CMDHB Governance	Last Review Date :	10/06/2020
Document Owner:	Chief Medical Officer (CMO) - Executive Management	Next Review Date:	10/06/2022
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	10/07/2019
If you are not reading this document directly from the Document Directory this may not be the most current version			

Adverse Event Checklist

Report due for completion: _____

Open Disclosure			
Within 24 hours	Name of Manager/Clinician	Date	Signature
Appropriate manager/clinician open disclosure to family and invitation to participate			
Patient/Family wish to participate	Yes / No		

Establish Investigation Team			
Title	Name of Person and Title	Date	Signature
Team Leader			
Clinical Opinion1			
Clinical Opinion2			
Other			
Other			
Other			
Other			
Other			
Other			

Staff Involved			
Code Name e.g. Dr A Midwife/RN 1.	Name of Person and Title	Interview Date	Interviewer

released under Official Information Act - ref OIA 23062020 Van Vliet Lovatt

10Document ID:	A1136626	CMH Revision No:	1.0
Service:	CMDHB Governance	Last Review Date :	10/06/2020
Document Owner:	Chief Medical Officer (CMO) - Executive Management	Next Review Date:	10/06/2022
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	10/07/2019
If you are not reading this document directly from the Document Directory this may not be the most current version			

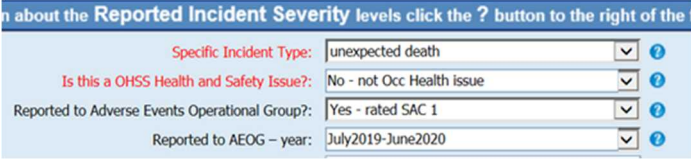

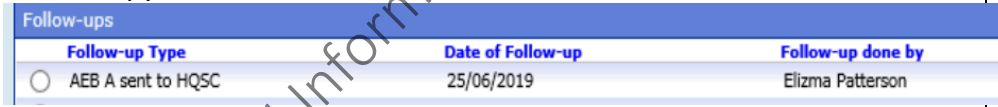
RCA Report			
	Date Sent	Date Approval Received	Signature
Draft Report Agreed by Investigation Team			
Report sent to staff involved to verify factual content and recommendations			
Final Report Agreed by Investigation Team			
Send Final Report to Corporate Lawyer if required			
Present Final Report at AEOG and Obtain sign off			
Offer meeting to Patient/Family to discuss report			
Send Final Report to Patient/Family if appropriate			

Final Documentation Requirements		
	Date	Signature
Update relevant organisational system to record and monitor recommendation follow-up		

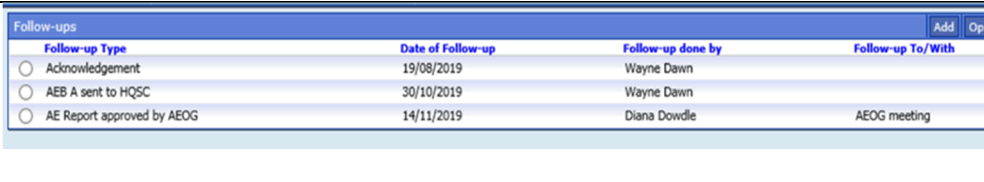


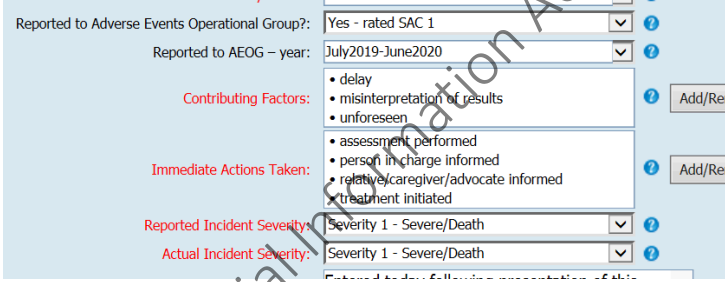
released under Official Information Act - ref OIA 23062020 Van Wey Lovatt

10Document ID:	A1136626	CMH Revision No:	1.0
Service:	CMDHB Governance	Last Review Date :	10/06/2020
Document Owner:	Chief Medical Officer (CMO) - Executive Management	Next Review Date:	10/06/2022
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	10/07/2019
If you are not reading this document directly from the Document Directory this may not be the most current version			

Feedback Central Adverse Events Process

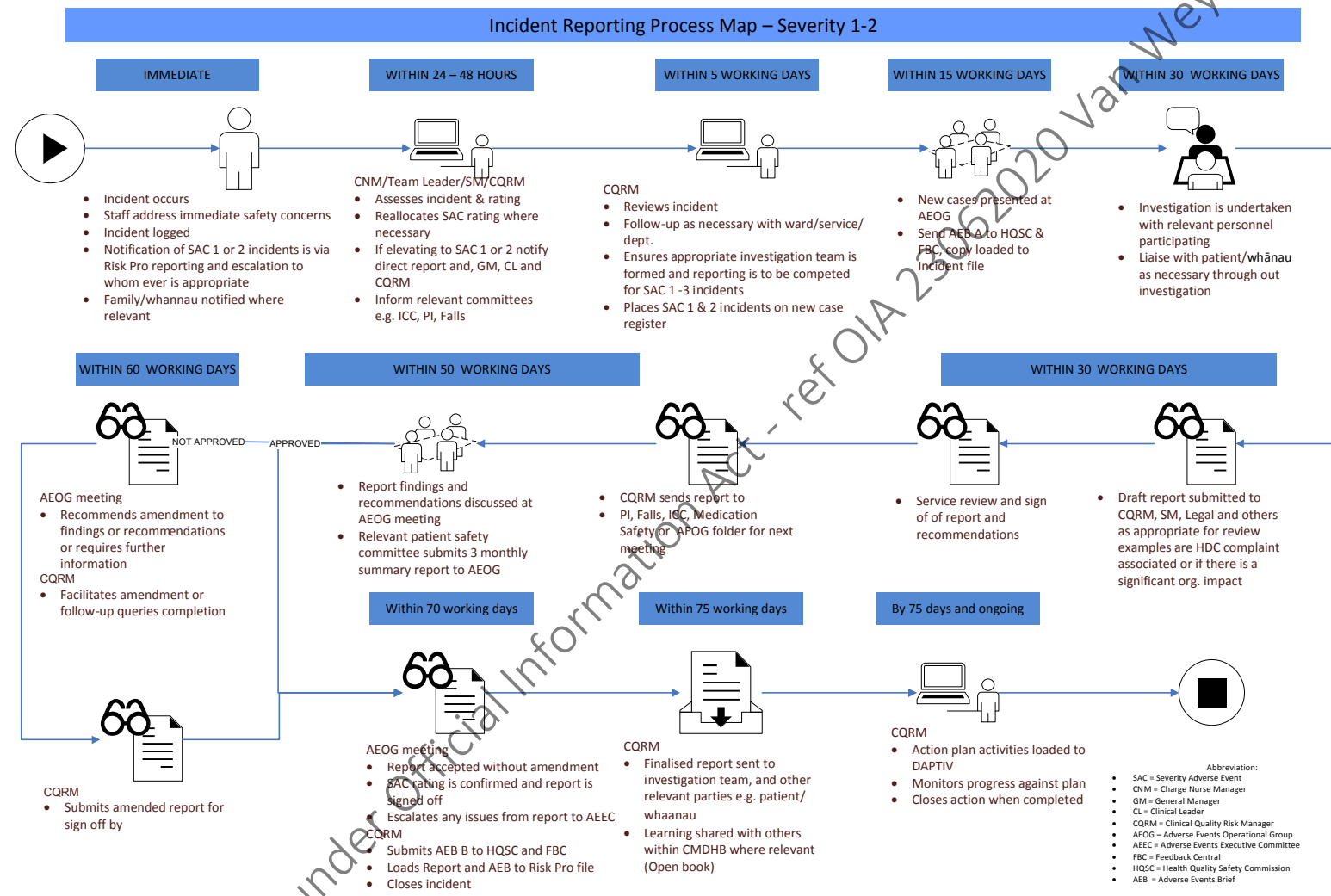
Adverse Event Operational Group (AEOG) Processes Checklist	
Key: Feedback Central -FC/ Clinical Quality Risk Manager -CQRM	
Actions	Person
Identified new incidents SAC 1 & 2 / Always Report & Review (ARR) updated on new case register for AEOG agenda <i>Workgroup/AEC/AE Operational Group/Pre AE meeting/New cases register</i>	CQRM
Update new cases in RMPRO file Specific Incidents Details <i>Reported to Adverse Events Operational Group- SAC rating & AEOG year</i> 	CQRM
Update new cases in RMPRO file after approved by AEOG meeting <i>RMPRO/Follow up List/ Meeting/ AEOG meeting new case</i> 	FC
Remove case from new case register once in RMPRO file Refresh new case register for next AEOG meeting date	FC
AEOG approved AEB A – submit online to HQSC. Send copy to Feedbackcentral@middlemore.co.nz Update RMPRO file <i>RMPRO/Follow up list/ AEB A sent to HQSC</i> Attach copy of AEB A form 	CQRM
Complete monthly report for AEB As sent to HQSC (<i>1st of the month</i>). Send to David Hughes, Deputy CMO <i>Workgroup/AEC/AE Operational Group/AEB's-HQSC/monthly AEB A report</i>	FC
Final Report to AEOG meeting + outcome	
Reports presented to AEOG meeting for sign off saved in folder for AEOG agenda <i>Workgroup/AEC/AE Operational Group/Pre AE meeting/ AE Reports for sign off</i>	CQRM
Reports approved by AEOG. Update RMPRO file- Report approved /date/ SAC rating confirmed <i>RMPRO/Follow up List</i>	FC

10Document ID:	A1136626	CMH Revision No:	1.0
Service:	CMDHB Governance	Last Review Date :	10/06/2020
Document Owner:	Chief Medical Officer (CMO) - Executive Management	Next Review Date:	10/06/2022
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	10/07/2019
If you are not reading this document directly from the Document Directory this may not be the most current version			

	
<p>AEOG approved AEB B –send to HQSC and copy to Feedbackcentral@middlemore.co.nz Update RMPPro file / Follow up list/ AEB B sent to HQSC / Attach copy of AEB B form</p> 	CQRM
<p>Final Report</p>	
<p>Approved Final Report (de-identified) & Action Plan– Send to Chairperson of AEOG email Feedbackcentral@middlemore.co.nz</p>	CQRM
<p>Chairperson sign and date final report. Send back to CQRM for copy. Save in <i>Workgroup/AEC/AE Operational Group/AE Completed Incident Reports</i></p>	Chair/ FC
<p>Update RMPPro file- Attach final signed report (PDF) with action plan RMPPro/Follow up List/ AE Report approved by AEOG</p> 	FC
<p>Update RMPPro file Specific Incidents Details. Reported to Adverse Events Operational Group- SAC rating & Actual Incident severity</p> 	
<p>Action Plans</p>	
<p>Corrective action plan up loaded into Daptiv</p>	CQRM
<p>Add case to HAC draft version <i>AEC/ HAC monthly report</i> -Includes to SAC 1 & 2 / Always Report & Review events. Excluding Mental Health. Number of Falls</p>	FC

10Document ID:	A1136626	CMH Revision No:	1.0
Service:	CMDHB Governance	Last Review Date :	10/06/2020
Document Owner:	Chief Medical Officer (CMO) - Executive Management	Next Review Date:	10/06/2022
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	10/07/2019
If you are not reading this document directly from the Document Directory this may not be the most current version			

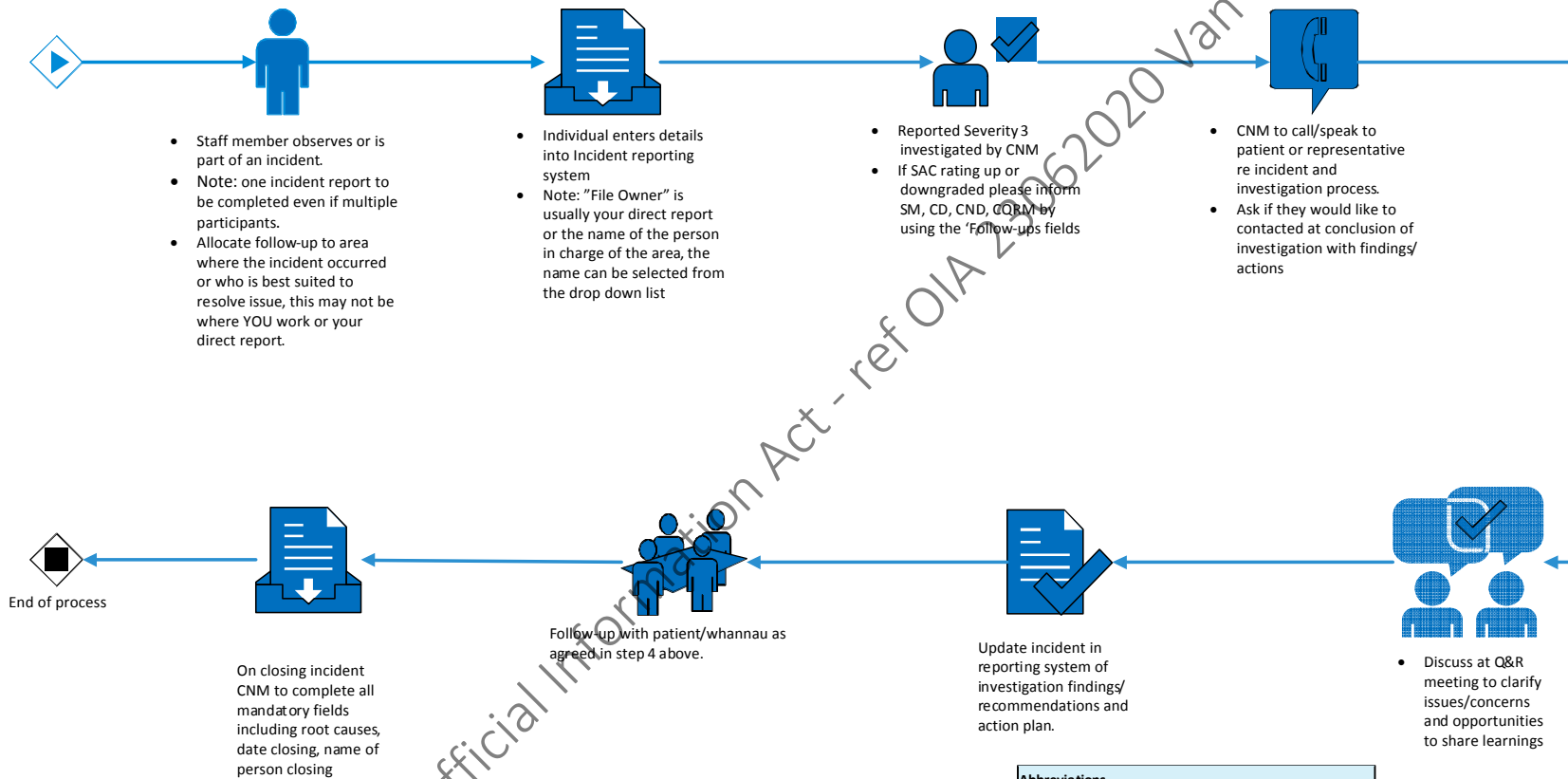
Appendix 1



Document ID:	A1136626	CMH Revision No:	1.0
Service:	CMDHB Governance	Last Review Date :	10/06/2020
Document Owner:	Chief Medical Officer (CMO) - Executive Management	Next Review Date:	10/06/2022
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	dd/mm/yyyy

If you are not reading this document directly from the Document Directory this may not be the most current version

Incident Reporting Process Map – Severity 3



Abbreviations
 GM = General Manager,
 CL = Clinical Director
 CND = Clinical Nurse Director
 CORM = Clinical Quality and Risk Manager
 QR = Quality Facilitators
 AE = Adverse Events

Document ID:	A1136626	CMH Revision No:	1.0
Service:	CMDHB Governance	Last Review Date :	10/06/2020
Document Owner:	Chief Medical Officer (CMO) - Executive Management	Next Review Date:	10/06/2022
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	dd/mm/yyyy

If you are not reading this document directly from the Document Directory this may not be the most current version

Policy: Privacy – Protecting and respecting personal information

Overview

The right to privacy refers to having control over your personal information. It is the ability to limit who can collect this information, how this information is kept and what can be done with it.

Counties Manukau Health (CM Health) recognises the importance of protecting personal information about our staff and patients in all business activities. Protecting an individual’s privacy is about respecting a person’s rights and is fundamental to maintaining trust and freedom of expression.

Contents

Scope	2
Objective	2
Legislation and Scope	2
Associated Documents	2
Definitions.....	3
Compliance with the Act and Policy	3
Patients	4
Staff Information	4
Corporate Records.....	4
Non-Compliance.....	5
Change/New Systems/ Processes – Privacy Impact Assessments	5
Sharing personal information with other agencies	5
Sensitive information.....	5
Unique identifiers.....	7
Roles and Responsibilities.....	7
Policy Updates.....	7
Associated Documents and References.....	7
Appendix 1 – Privacy Act Principles.....	8
Appendix 2 - Roles and Responsibilities	11

Document ID:	A598070	CMH Revision No:	1.0
Division:	Executive Management	Last Review Date :	12/12/2016
Document Owner:	Risk and Privacy Manager -Strategic Development	Next Review Date:	1/10/2018
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	01/03/2004
Counties Manukau Health			

Scope All employees, contractors and volunteers who have access to information about identifiable individuals ('personal information') must comply with this policy and related procedures.

Objective The objectives of this policy are to:

- Provide guidance and confirm our expectations as to the management of personal information, including the collection; storage; use of; retention and destruction, and how to deal with complaints and potential breaches of privacy obligations.
- Outlining our compliance requirements with the Privacy Principles as defined in the Privacy Act 1993 and Health Information Privacy Code.

Legislation and Scope The Privacy Act 1993 and related Health Information Privacy Code provides the foundation for managing personal information and health information (information relating to the health or disability of a person). The Act provides guidance on managing all personal information whereas the Health Information Privacy Code specifically addresses the management of health information. The Act and the Code respectively provide compliance guidance through 12 privacy principles. Personal and health information relating to identifiable individuals must be managed according to the Act and Code, on which this policy is based.

The scope of this policy covers all personal information as defined by the Privacy 1993, and includes information relating to staff, patients, visitors and contractors.

This policy applies to all persons working within CM Health, or using CM Health facilities – including staff, managers and contractors, volunteers and independent practitioners who provide services under access agreements, students, external personnel and Board members. All individuals are required to familiarise themselves with the contents of this policy, the privacy principles and the Health Information Privacy Code.

Associated Documents

This policy is to be read in conjunction with the various policies, procedures and guidelines to support the delivery of expectations, referenced within this policy document. Additional procedures and guidelines may be added and will be stored on the Privacy Intranet site.

Document ID:	A598070	CMH Revision No:	1.0
Division:	Executive Management	Last Review Date :	12/12/2016
Document Owner:	Risk and Privacy Manager -Strategic Development	Next Review Date:	1/10/2018
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	01/03/2004
Counties Manukau Health			

Definitions

The following definitions apply:

Personal information	Information about an identifiable individual; and includes information relating to a death that is maintained by the Registrar-General pursuant to the Births, Deaths, Marriages, and Relationships Registration Act 1995 , or any former Act (as defined by the Births, Deaths, Marriages, and Relationships Registration Act 1995) Privacy Act 1993. Personal information includes images and may be a photo, video recording or audio recording, and includes images of a pathology report or diagnostic image.
Privacy	The common understanding of privacy is that: <ul style="list-style-type: none"> • People need to be able to protect information about themselves • People need to be able to restrict who they share their personal information with
Office of the Privacy Commissioner	The regulator works to develop and promote a culture in which personal and health information is protected and respected, through the administration of the Privacy Act 1993. The Privacy Act is New Zealand's main privacy law. It mostly governs personal and health information about individual people, though the Privacy Commissioner also has a wider ability to consider developments or actions that affect personal privacy.

Compliance with the Act and Policy

You are required to adhere to the following policy requirements:

- All staff dealing with personal information should comply with this policy, the privacy principles; refer Appendix 1 and the associated procedures relating to privacy and information management. This should include all interactions with staff, patients and third parties.
- All affected individuals must observe the legal requirements concerning access, disclosure, accuracy, retention and destruction and correction of personal information.
- Personal information should only be accessed if this is required to execute the tasks related to your job.
- For staff accessing their own family, friends and relatives, this should be performed using the Staff Portal, with the appropriate approval.
- All breaches of privacy are to be reported through the Incident Reporting process for assessment and if necessary investigation by the Privacy Officer.

Document ID:	A598070	CMH Revision No:	1.0
Division:	Executive Management	Last Review Date :	12/12/2016
Document Owner:	Risk and Privacy Manager -Strategic Development	Next Review Date:	1/10/2018
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	01/03/2004
Counties Manukau Health			

Patients

- Have rights over information about themselves (health information). They have the right to access information about themselves and the right to seek correction of that information if they think it is inaccurate or misleading.
- Expect their health information to be kept confidential.
- Expect their health information to be treated as sensitive.
- Expect their health information may have on-going use if a piece of clinical information becomes relevant to their care even a long time after it was initially collected
- Expect their health information will be used for the purpose for which it was initially collected and they will be told about that purpose.

Staff Information

- All forms of employee records including hard copy and electronic records are protected and correct procedures are carried out in relation to the handling and management of employee records and files by any employee with access to employee information including but not limited to Managers, Human Resources, Recruitment and healthAlliance payroll employees in accordance with the Employee Records Policy and with the Privacy Act 1993.
- An employee's personal information is to be treated at all times as private and confidential and only disclosed in accordance with the Privacy Act and other relevant legislation.
- Breach of employee confidentiality regarding disclosure of any employee's personal information, or inappropriate use of that information may constitute serious misconduct and result in disciplinary action.
- An employee's personal information may only be accessed by authorised employees as outlined in the Employee Records policy.
- Employees have the right to access any information about, or regarding them, held by Counties Manukau Health in accordance with Principle 6 of the Privacy Act 1996. Such access follows procedures outlined in the Employee Records Policy and may be subject to some restrictions in line with the Privacy Act 1993.

Corporate Records

- Where patient or staff identifiable information is stored within the Enterprise Content Management system, that information must be secured and only be accessible by authorised persons.

Refer to the Corporate Information Management Policy (Doc. A11532) for further information.

Document ID:	A598070	CMH Revision No:	1.0
Division:	Executive Management	Last Review Date :	12/12/2016
Document Owner:	Risk and Privacy Manager -Strategic Development	Next Review Date:	1/10/2018
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	01/03/2004
Counties Manukau Health			

Non-Compliance

Breaches of this Privacy Policy may be considered serious misconduct and the staff members involved may be subject to disciplinary proceedings. Any privacy breaches which also realise an interference with a person's privacy may see CM Health liable for fines and penalties and/or to pay compensation.

Change/New Systems/ Processes – Privacy Impact Assessments

When a substantial change to a workflow is contemplated, whether due (for example) to the design of a new process, the introduction of a new IT system or making systemic changes, the project team must evaluate whether a Privacy Impact Assessment is required. This allows the project team to assess the potential risk of new or changed privacy risks to the organisation, the mitigations proposed and how to manage any on-going residual risk.

All Privacy Impact Assessments must be reviewed and endorsed by the Privacy Officer and Deputy Chief Information Officer at a minimum. For projects with significant changes or high privacy risks, the Privacy Impact Assessment will also be reviewed and endorsed by the Privacy Committee, with all Privacy Impact Assessments approved by the individual business Project Sponsors or associated Steering Committees, as appropriate.

All Privacy Impact Assessments must be signed off and approved by the relevant business owner prior to submission for review and any necessary endorsement from the Privacy Committee.

The Privacy Impact Assessment must be approved and finalised before Go-Live.

For regional projects, approval needs to be provided by a CM Health staff member, with the appropriate level of authority, with the Privacy Impact Assessment reviewed and assessed by the Regional Privacy Advisory Group.

The Privacy Impact Assessment must be completed on the regional template.

The Office of the Privacy Commissioner's website contains some useful guidance around when a Privacy Impact Assessment is needed.

<https://www.privacy.org.nz/>

Sharing personal information with other agencies

Where CM Health is working jointly with other agencies for a set purpose and the sharing of personal information is required, the team needs to assess whether at a minimum a Memorandum of Understanding (MOU) is required to formalise governance processes for the protection of this information. The Privacy Officer must be notified when CM Health intends to enter into on-going information sharing arrangements with other/ multi-agencies.

Sensitive information

All personal information needs to be protected and respected, but certain records are considered to be more sensitive than others, including but not limited to

Document ID:	A598070	CMH Revision No:	1.0
Division:	Executive Management	Last Review Date :	12/12/2016
Document Owner:	Risk and Privacy Manager -Strategic Development	Next Review Date:	1/10/2018
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	01/03/2004
Counties Manukau Health			

mental health information; sexual orientation or data related thereto; certain aspects of women's health for example termination of pregnancy; etc. Staff need to assess the sensitivity of the information in the context of the situation and the individual and ensure that the information is safeguarded appropriately.

released under Official Information Act - ref OIA 23062020 Van Wey Lovatt

Document ID:	A598070	CMH Revision No:	1.0
Division:	Executive Management	Last Review Date :	12/12/2016
Document Owner:	Risk and Privacy Manager -Strategic Development	Next Review Date:	1/10/2018
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	01/03/2004
Counties Manukau Health			

Unique identifiers

CM Health assigns and uses the National Health Index number to identify patients. Unique identifiers are also assigned to staff members to support the identification of the individual. The unique identifiers are used to support CM Health to carry out its function of patient care and staff management, with disclosure aligned to purpose of collection.

Roles and Responsibilities

Protecting personal and health information across CM Health requires the support and vigilance from all staff. Some roles and responsibilities are defined in Appendix 2.

Policy Updates

All policy changes impacting privacy must be reviewed by the Privacy Committee before being submitted for approval at the respective committees.

Associated Documents and References

The following associated documents and references are applicable:

NZ Legislation

Privacy Act 1993
Health Information Privacy Code 1994
Official Information Act 1982
Health Act 1956
Public Records Act 2005
Vulnerable Children Act 2014

CM Health Board Policy

All CMDHB health information related policies, procedures and guidelines

Other Related Documents

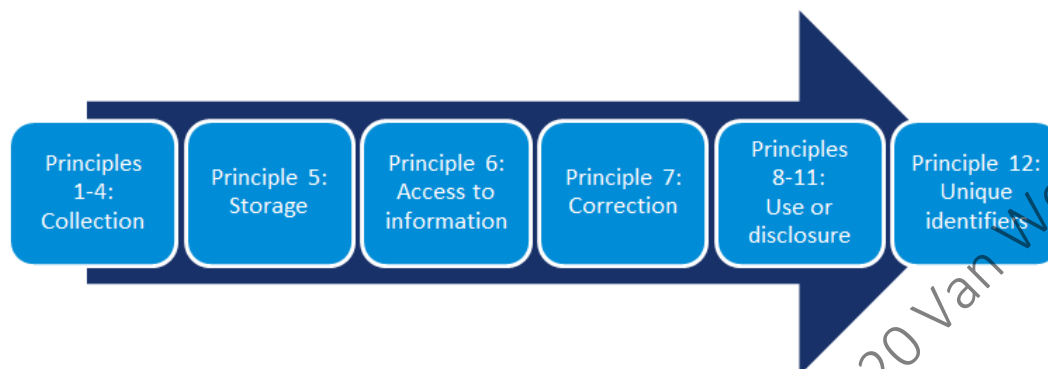
SouthNET – Privacy Intranet Site

Document ID:	A598070	CMH Revision No:	1.0
Division:	Executive Management	Last Review Date :	12/12/2016
Document Owner:	Risk and Privacy Manager -Strategic Development	Next Review Date:	1/10/2018
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	01/03/2004
Counties Manukau Health			

Appendix 1 – Privacy Act Principles

To protect and respect personal information, the following principles apply:

Note that the principles apply to personal information relating to staff, patients, visitors and contractors



Principle 1 – Only collect personal information if you really need it

Personal information must only be collected when:

- The collection is for a lawful purpose, connected with what the agency does, and
- It is necessary to collect the information for that purpose

Principle 2 – Get it straight from the people concerned where possible

Personal information must usually be collected from the person the information is about. But sometimes it is all right to collect information from other people instead – for instance when:

- Getting it from the person concerned would undermine the purpose of the collection
- The person is unable to provide the information at the time collection is necessary. The person concerned authorises collection from someone else

Principle 3 – Tell them what you’re going to do with it

When an agency collects personal information from the person the information is about, it has to take reasonable steps to make sure that person knows things like:

- Why it is being collected
- Who will get the information
- Whether the person *has* to give the information or whether this is voluntary
- What will happen if the information isn’t provided

Sometimes there are good reasons for not letting a person know about the collection, for example, if it would undermine the purpose of the collection, or it’s just not possible to tell the person.

Document ID:	A598070	CMH Revision No:	1.0
Division:	Executive Management	Last Review Date :	12/12/2016
Document Owner:	Risk and Privacy Manager -Strategic Development	Next Review Date:	1/10/2018
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	01/03/2004
Counties Manukau Health			

Principle 4 – Collect it legally and fairly

Personal information must not be collected by unlawful means or by means that are unfair or unreasonably intrusive in the circumstances.

Principle 5 – Take care of it once you have got it

It's impossible to stop all mistakes. But agencies must ensure that there are reasonable safeguards in place to prevent loss, misuse or disclosure of information.

Principle 6 – People can see their personal information if they want to

People usually have a right to ask for access to that personal information.

However, sometimes agencies can refuse to give access to information, for instance because giving the information would:

- Endanger a person's safety
- Prevent detection and investigation of criminal offences
- Involve an unwarranted breach of someone else's privacy

Principle 7 – They can correct it if it is wrong

People have a right to ask the agency to correct information about them if they think it is wrong. If the agency does not want to correct the information, it does not usually have to. But people can ask the agency to add *their* views to the record about what the correct information is.

Principle 8 - Make sure personal information is correct before you use it

Before it uses or discloses personal information an agency must take reasonable steps to check that information is accurate, complete, relevant, up-to-date and not misleading.

Principle 9 – Get rid of it when you are done with it

An agency that holds personal information must not keep that information for longer than is necessary for the purposes for which the information may be lawfully used.

Principle 10 - Use it for the purpose you got it

Agencies must use personal information for the same purpose for which they collected that information. Other uses are occasionally permitted, for example because this is necessary to enforce the law, or the use is directly related to the purpose for which the agency got the information.

Principle 11 - Only disclose it if you have a good reason

Agencies can only disclose personal information in limited circumstances. An agency can disclose information if it reasonably believes, for example that:

- Disclosure is one of the purposes for which the agency got the information
- Disclosure is necessary to prevent or lessen a serious threat to the life or health of the individual

Document ID:	A598070	CMH Revision No:	1.0
Division:	Executive Management	Last Review Date :	12/12/2016
Document Owner:	Risk and Privacy Manager -Strategic Development	Next Review Date:	1/10/2018
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	01/03/2004
Counties Manukau Health			

concerned or another individual

- Disclosure is necessary for court proceedings
- The person concerned authorised the disclosure
- The information is going to be used in a form that does not identify the person concerned.

Principle 12 - Only assign unique identifiers where permitted

Some agencies give people a 'unique identifier' instead of their name. Examples are driver's license number; IRD numbers, bank client numbers and passport numbers. An agency cannot use the unique identifier given to a person by another agency. People are not required to disclose their unique identifier unless this is one of the purposes for which the unique identifier was set-up (or directly related to those purposes).

Document ID:	A598070	CMH Revision No:	1.0
Division:	Executive Management	Last Review Date :	12/12/2016
Document Owner:	Risk and Privacy Manager -Strategic Development	Next Review Date:	1/10/2018
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	01/03/2004
Counties Manukau Health			

Appendix 2 - Roles and Responsibilities

Protecting personal information across CM Health requires the support and vigilance from all staff. Some roles and responsibilities are defined below:

Individual	Accountability
All Staff (includes volunteers and contractors)	<ul style="list-style-type: none"> Understand and ensure compliance with the privacy principle requirements, managing personal information safely and with integrity. Respect others' information and be mindful when discussing personal information that this is appropriate and in the correct forum. Be familiar with CM Health's privacy policies and procedures.
Chief Information Officer	<ul style="list-style-type: none"> Responsible for implementing security functions to ensure electronic health information is adequately secured against loss and protected against unlawful access, misuse and disclosure.
Clinical Governance Group	<ul style="list-style-type: none"> Responsible for setting, maintaining and monitoring privacy standards. Receives reports from the Privacy Committee.
Corporate Records	<ul style="list-style-type: none"> Responsible for the management of corporate records, with consideration for privacy and security. Responsible for ensuring information is stored securely and appropriately with access restricted to an as-needs basis.
Executive Leadership Team	<p>Responsible for:</p> <ul style="list-style-type: none"> Managing privacy awareness within their respective directorates. Responsible for the governance and accountability of the District Health Board in relation to privacy and the Government's Chief Privacy Officer's expectations.
General Managers	<p>Via their Service Managers:</p> <ul style="list-style-type: none"> Are responsible for the identification and initial response to privacy breaches. Report all breaches or near misses through the formal incident reporting process. Where allocated, investigate the cause of the breach and provide recommendations for remediation. Notification of the privacy breach or near miss to the Privacy Officer.
Human Resources	<ul style="list-style-type: none"> Manage and safeguard staff records, include appropriate storage; user access and use. Responsible to manage the disciplinary process, where required as defined by CM Health's internal policies.

Document ID:	A598070	CMH Revision No:	1.0
Division:	Executive Management	Last Review Date :	12/12/2016
Document Owner:	Risk and Privacy Manager -Strategic Development	Next Review Date:	1/10/2018
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	01/03/2004
Counties Manukau Health			

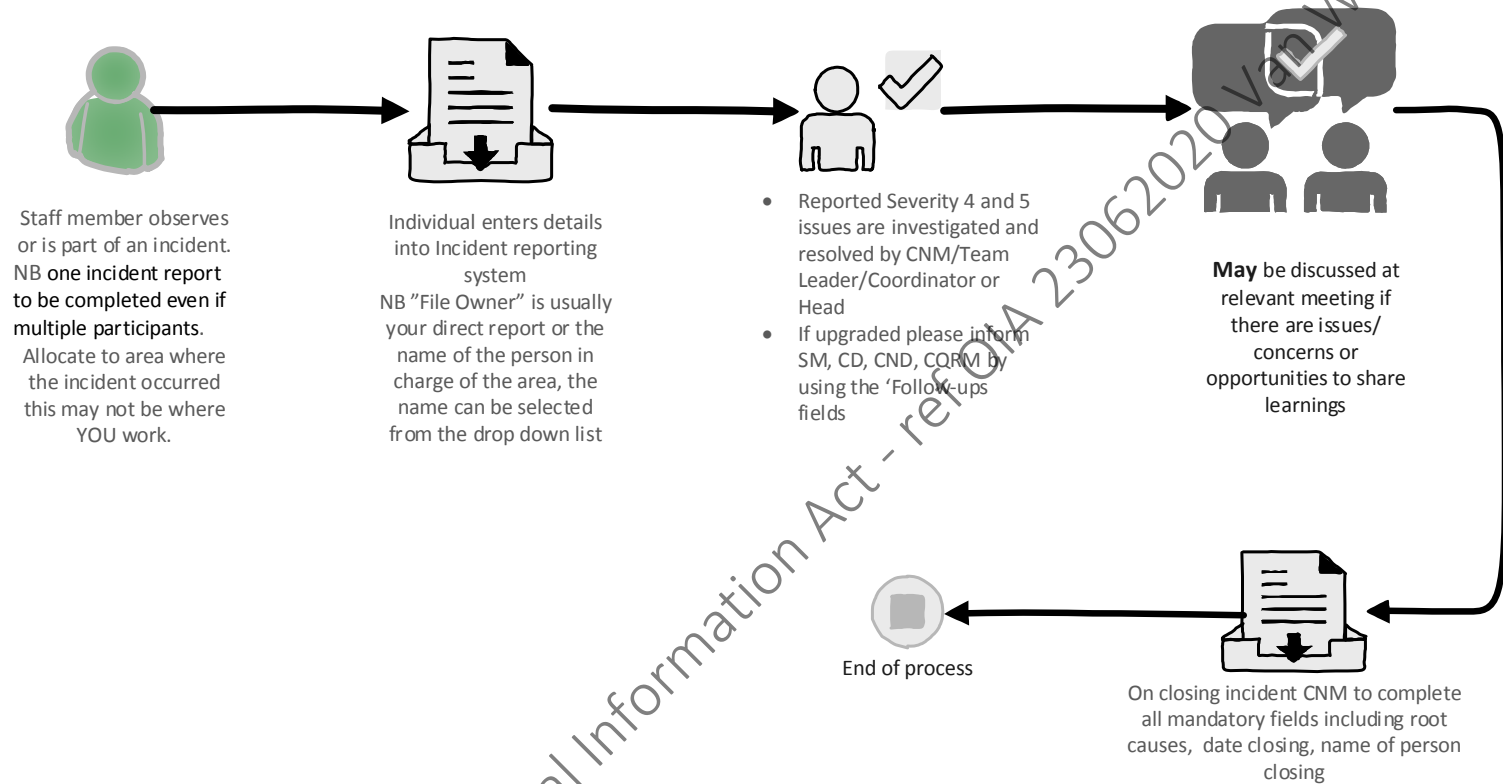
Individual	Accountability
Legal Team	<p>Responsible for:</p> <ul style="list-style-type: none"> • Providing legal advice on the interpretation and application of the Privacy Act and Health Information Privacy Code. • Providing legal representation on the Privacy Committee and Health Information Committee. • Supporting the Risk and Privacy Manager in their role as Privacy Officer. • Ensuring the DHB's policies and procedures comply with the Act and Code and other relevant legislation, including any amendments, legal developments and case law.
Privacy Committee	<p>The role of the Committee is to:</p> <ul style="list-style-type: none"> • Direct and oversee the implementation of Counties Manukau Health's Privacy Strategy. • Lead the development and implementation of policies, procedures, guidelines and security measures that aim to protect personal information, including health information. • Direct and oversee the implementation of measures to ensure that personal information is managed in accordance with all relevant legislation as well as Counties Manukau Health's policies and procedures. • Review and provide advice in relation to privacy related reports including summary or trend reports relating to privacy KPIs or privacy breach management. • Lead the development and implementation of privacy related training and education across Counties Manukau Health <p>The Committee is responsible for:</p> <ul style="list-style-type: none"> • Supporting Counties Manukau Health to meet its legal obligations under the Privacy Act 1993 and Health Information Privacy Code 1994; • Promoting good privacy management practices across Counties Manukau Health; • Providing oversight of Counties Manukau Health's privacy practices; • Actively informing improvements on privacy management across Counties Manukau Health; and • Ensuring a consistent approach is taken to privacy related matters across Counties Manukau Health.
Patient Information Service	<p>Responsible for/ to:</p> <ul style="list-style-type: none"> • Perform user access reviews to ascertain appropriateness of access.

Document ID:	A598070	CMH Revision No:	1.0
Division:	Executive Management	Last Review Date :	12/12/2016
Document Owner:	Risk and Privacy Manager -Strategic Development	Next Review Date:	1/10/2018
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	01/03/2004
Counties Manukau Health			

Individual	Accountability
	<ul style="list-style-type: none"> The release of patient information as per CM Health's procedures. Escalate any technical patient information release issues or enquiries to the Privacy Officer or Legal Team for further consultation, as required.
Risk and Privacy Manager	<ul style="list-style-type: none"> Chair of the Privacy Committee. Acts as the organisation's Privacy Officer Responsible for the privacy policy, strategy and programme of work. Protects and promotes privacy by encouraging compliance with the Privacy Act and related Health Information Privacy Code. Conduct privacy incident investigations as necessary, and prepare investigation summary reports. Analyse breach information to assess organisational impact, if applicable. Responsible to communicate and consult on significant breaches with the Chief Medical Officer and Legal Team, as appropriate. Responsible for reporting to Executive Leadership Team, Clinical Governance Group and Audit, Risk and Finance Committee. Oversee external and internal communication and information sharing in the event of a privacy breach or incident. Manage external relationship with Government Chief Privacy Officer and the Office of the Privacy Commissioner.
Quality Managers/ Patient Care Advisors	<ul style="list-style-type: none"> Support adherence to policy and procedure Provide reports on breaches and near misses to Privacy Committee and other relevant stakeholders.
Research Committee/ Office	<ul style="list-style-type: none"> Responsible for the consideration of privacy and ethical aspects of research and audit conducted at Counties Manukau Health.
Service Managers	<ul style="list-style-type: none"> Responsible for the identification and initial response to privacy breaches. Report all breaches or near misses through the formal incident reporting process. Where allocated, investigate the cause of the breach and provide recommendations for remediation. Notification of the privacy breach or near miss to the Privacy Officer.

Document ID:	A598070	CMH Revision No:	1.0
Division:	Executive Management	Last Review Date :	12/12/2016
Document Owner:	Risk and Privacy Manager -Strategic Development	Next Review Date:	1/10/2018
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	01/03/2004
Counties Manukau Health			

Incident Reporting Process Map – Severity 4-5



Abbreviation
 GM = General Manager,
 CL = Clinical Director
 CND = Clinical Nurse Director
 CQRM = Clinical Quality and Risk Manager

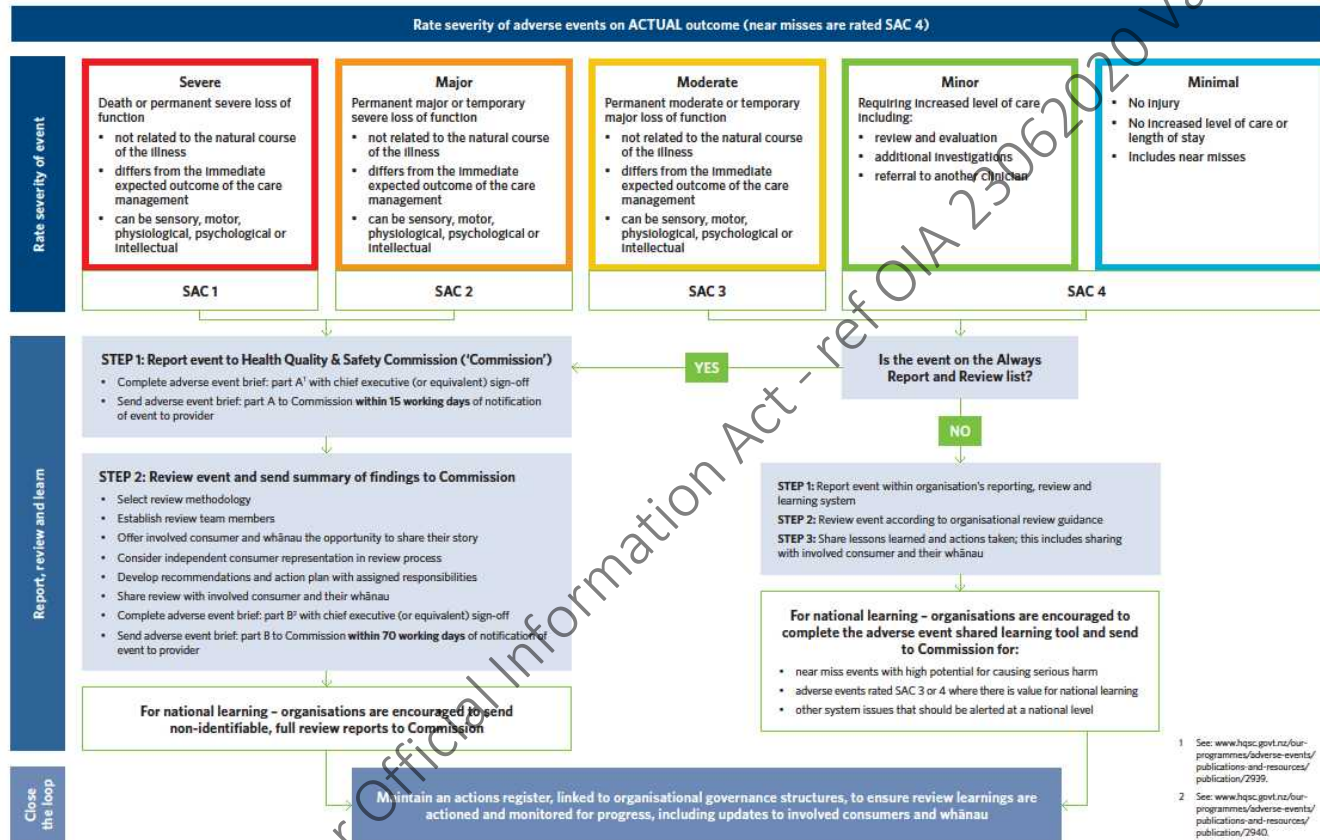
Guiding Documents
[Complaints Resolution and Management and Patient Feedback Procedure](#)
[Incident Reporting and Investigation - Policy](#)

Document ID:	A1136626	CMH Revision No:	1.0
Service:	CMDHB Governance	Last Review Date :	10/06/2020
Document Owner:	Chief Medical Officer (CMO) - Executive Management	Next Review Date:	10/06/2022
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	dd/mm/yyyy

If you are not reading this document directly from the Document Directory this may not be the most current version

Appendix 2 SAC rating and assessment

Severity Assessment Code (SAC) rating and triage tool for adverse event reporting



Document ID:	A1136626	CMH Revision No:	1.0
Service:	CMDHB Governance	Last Review Date :	10/06/2020
Document Owner:	Chief Medical Officer (CMO) - Executive Management	Next Review Date:	10/06/2022
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	dd/mm/yyyy

If you are not reading this document directly from the Document Directory this may not be the most current version

Procedure: Managing privacy breaches

Overview

A privacy breach is when we do not comply with one or more of the Information Privacy Principles as defined in the Privacy Act 1993 or the Health Information Privacy Code 1994.

If we fail to comply with the principle of disclosure, this results in a breach – the disclosure of personal information to the incorrect or unauthorised individual. Even with the best of intentions breaches happen. Breaches occur through loss or leaking of personal information through complacency, inadequate security, poor procedures or rare accidents. The ease of digital copying and transmission means that the data breaches can range from the loss of one person’s information to hundreds of thousands of records. The cause of a breach can be accidental or through the deliberate actions of others.

It is vital for the protection of CM Health’s reputation and its relationship with the people who entrust their information to us that we do everything we can to prevent a breach from happening. Should a breach occur, it is important to do everything we can to minimise the harm that it might cause and any likelihood of a reoccurrence.

This procedure provides guidance to help staff prevent common mistakes that lead to privacy and breaches and the steps to follow should a breach occur.

Contents

Purpose 2

What is a privacy breach?..... 2

How do breaches happen? 2

What is ‘breach notification’?..... 2

Four key steps on how to respond to breaches..... 3

Near misses..... 3

Disciplinary action..... 4

Associated Documents and References 4

References..... 4

Appendix A – Four key steps on how to respond to breaches..... 5

Appendix B – Reporting and Escalation Matrix..... 12

Appendix C - Guideline for logging a breach within the Incident Management System 16

Appendix D – Notification Template 18

Document ID:	A321063	CMH Revision No:	2.0
Division:	Executive Management	Last Review Date :	1/03/2018
Document Owner:	Risk and Privacy Manager -Strategic Development	Next Review Date:	28/02/2021
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	01/04/2014
Counties Manukau District Health Board			

Purpose

The purpose of this procedure is to specify how a breach of privacy in relation to patient or staff information should be managed. This procedure should be read in conjunction with ‘Policy: [Privacy – Protecting and respecting personal information](#)’.

What is a privacy breach?

A privacy breach is when CM Health does not comply with one or more of the Information Privacy Principles set out in section 6 of the Privacy Act 1993 (or Health Information Privacy Code 1994). A breach of a privacy principle can occur with/ without causing harm to an individual.

How do breaches happen?

Some of the most common breaches happen when personal information of customers, patients, clients or employees is stolen, lost or mistakenly disclosed. A breach may also be a consequence of faulty business procedure or an operational break-down.

Breaches happen in a number of ways. Some common examples include:

- Lost or stolen laptops, removable storage devices, or paper records containing personal information
- Computer hard disk drives being thrown away, recycled or returned to leasing companies or serviced incorrectly, without the content first being erased
- Databases of personal information being hacked or illegally accessed by others outside the agency or organisation
- Employees accessing or disclosing personal information outside their authorisation
- Paper documents taken from recycling or rubbish bins or not appropriately discarded
- Personal information given to the wrong person by sending information to the wrong physical or email address
- Releasing personal information to a person who is fraudulently pretending to be someone else

What is ‘breach notification’?

Breach notification is the practice of notifying affected individuals and the Privacy Commissioner when their personal information has become available to unauthorised individuals or organisations. This enables those affected to take steps to prevent the misuse of their details.

Document ID:	A321063	CMH Revision No:	2.0
Division:	Executive Management	Last Review Date :	1/03/2018
Document Owner:	Risk and Privacy Manager -Strategic Development	Next Review Date:	28/02/2021
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	01/04/2014
Counties Manukau District Health Board			

Four key steps on how to respond to breaches

There are four key steps in dealing with a breach:

1. Contain the breach and make a first assessment

When a potential breach is identified, the service manager must be notified. The service manager must initiate an investigation and notify the Risk and Privacy Manager and their General Manager. Based on the severity of the breach, other individuals may be called upon to assist in the investigation.

Be sure to take each situation seriously and move immediately to investigate the potential breach.

Refer to Appendix A for further details and checklist.

2. Evaluate the risks

Consider the potential for harm to the individual to whom the data relates, harm to the public’s trust in CM Health and harm to our reputation.

3. Notify affected people if necessary

The Risk and Privacy Manager, in consultation with Legal where appropriate will decide on the notification requirements and allocation of responsibility for this.

Refer to Appendix B for escalation path calculation.

4. Prevent a repeat

Steps 1-3 must be undertaken either simultaneously or in quick succession. Step 4 provides recommendations for longer-term solutions and prevention strategies. The decision on how to respond should be made on a case-by-case basis.

All breaches must be reported in the Incident Management System.

Refer to Appendix C for some key steps to logging an incident.

Near misses

A near miss is an identified action that would have led to a privacy breach but did not because the information was not disclosed. It is expected that near misses will be dealt with in a similar way to potential

Document ID:	A321063	CMH Revision No:	2.0
Division:	Executive Management	Last Review Date :	1/03/2018
Document Owner:	Risk and Privacy Manager -Strategic Development	Next Review Date:	28/02/2021
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	01/04/2014
Counties Manukau District Health Board			

released under Official Information Act ref OIA 25062020 Van Wey Lovatt

breaches.

- Make an initial assessment of how the near miss occurred
- Evaluate the risks
- Establish the cause and extent of the near miss
- Consider who could have been affected by the near miss
- Consider what harm could have been caused
- Prevent a repeat.

Disciplinary action

A breach by a staff member may constitute serious misconduct, particularly where the breach has occurred because the staff member has failed to comply with CM Health’s policies for handling personal information. This may result in a disciplinary process with appropriate consequences (including dismissal where the circumstances justify it.)

Associated Documents and References

The following associated documents and references are applicable:

NZ Legislation

- [Privacy Act 1993](#)
- [Health Information Privacy Code 1994](#)
- [Official Information Act 1982](#)
- [Health Act 1956](#)
- [Public Records Act 2005](#)
- [Vulnerable Children Act 2014](#)

CM Health Board Policy

Policy: [Privacy – Protecting and respecting personal information](#).
All CMDHB health information policies, procedures and guidelines
Policy: [A Just Culture](#)

Other Related Documents

[Paanui – Privacy Intranet Site](#)

References

This procedure has been adapted from:

- The Office of the Privacy Commissioner’s ‘Data Safety Toolkit: Preventing and Dealing with Data Breaches’, May 2014.
- Reporting privacy breaches – Government Chief Privacy Officer – Department of Internal Affairs

Document ID:	A321063	CMH Revision No:	2.0
Division:	Executive Management	Last Review Date :	1/03/2018
Document Owner:	Risk and Privacy Manager -Strategic Development	Next Review Date:	28/02/2021
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	01/04/2014
Counties Manukau District Health Board			

released under Official Information Act - ref: 2020/00013062020 Jan-Way Lovatt

Appendix A – Four key steps on how to respond to breaches

CHECKLIST OF STEPS

STEP 1: Contain the breach and make a first assessment

<p>Once you have discovered a potential breach, you should quickly take common sense steps to stop the situation becoming worse:</p>	<p>Immediately contain the breach</p> <p>While you diagnose what went wrong, stop the unauthorised practice, try and get back the records, consider disabling the system that was breached, cancel or change the computer access codes and try to fix any weaknesses in the physical or electronic security.</p>
	<p>Service manager to lead the investigation</p> <p>The service manager is responsible to carry out the early investigation and make the first recommendations. Independence and objectivity should be front of mind in the selection of who leads the investigation. The severity of the breach may warrant a team of individuals being involved. This will be decided upon in consultation with the Risk and Privacy Manager, General Manager or Director of the specific area and Legal, as appropriate.</p>
	<p>Decide whether to put a team together that could include people from other areas</p> <p>This might include people from other agencies or other District Health Boards or those from outside who have the expertise to deal with the situation (for example IT analysts, risk advisors etc.)</p>
	<p>Decide who needs to know within CM Health</p> <p>Build up a list of those that need to be told. Allocate responsibility for communication, deciding on the milestones and affected parties/ stakeholders that should be included. The Risk and Privacy Manager, based on the severity of the breach, may notify the Chief Medical Officer and Chief Executive Officer. Consider whether insurers need to be informed, as well as internal auditors, Quality and Risk Managers and Legal Advisors. In conjunction with the Risk and Privacy Manager, consider whether the Privacy Commissioner should be advised of the breach.</p>
	<p>Notify the police if the breach appears to involve theft or other criminal activity. Be careful not to destroy evidence that may be needed by CM Health or the police in finding the cause of the</p>

Document ID:	A321063	CMH Revision No:	2.0
Division:	Executive Management	Last Review Date :	1/03/2018
Document Owner:	Risk and Privacy Manager -Strategic Development	Next Review Date:	28/02/2021
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	01/04/2014
Counties Manukau District Health Board			

	<p>problem or which might allow you to fix the issue</p> <hr/> <p>Log the breach into the Incident Management System.</p> <p>A summary of all privacy incidents logged into the Incident Management System will be provided to the Privacy Committee by the Risk and Privacy Manager.</p>
--	--

released under Official Information Act - ref OIA 23062020 Van Wey Lovatt

Document ID:	A321063	CMH Revision No:	2.0
Division:	Executive Management	Last Review Date :	1/03/2018
Document Owner:	Risk and Privacy Manager -Strategic Development	Next Review Date:	28/02/2021
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	01/04/2014
Counties Manukau District Health Board			

STEP 2: Evaluate the risks

Once you have discovered that a breach has occurred, you should quickly take common sense steps to stop the damage becoming worse:

<p>Find out what kind of personal information is involved</p> <p>The more sensitive the information, the higher the risk of harm to the people affected. Health information, driver's licence numbers and credit card details can all cause harm on their own but if used together it could be used for identify theft. A combination of personal information is typically more sensitive than a single piece of personal information.</p>
<p>What might that personal information show?</p> <p>For example, a list of customers on a newspaper delivery route may not be sensitive. But the same information about customers who have requested that their deliveries be stopped while on holiday would be useful information to criminals.</p>
<p>Is the personal information easy to get at?</p> <p>If the information is not password secured or encrypted, then there is a more real risk of it being misused.</p>
<p>What caused the breach?</p> <p>Try to find out what caused the breach and if there is a risk of more breaches.</p>
<p>What is the extent of the breach?</p> <p>Try and identify the size of the breach including the number and nature of the likely recipients as well as how many people's personal information has been lost. It is also important to identify the risk of the information being circulated further. Find out if the breach is the result of a systemic problem or an isolated incident.</p>
<p>Assess whether harm could result from the breach</p> <p>Consider this from the point of view of the people affected taking into account the reasonable expectations of the individual.</p> <p><i>Types of harm to the individual could include:</i></p> <ul style="list-style-type: none"> • Identity theft • Financial loss • Loss of business or employment opportunities • Significant humiliation • Loss of dignity

Document ID:	A321063	CMH Revision No:	2.0
Division:	Executive Management	Last Review Date :	1/03/2018
Document Owner:	Risk and Privacy Manager -Strategic Development	Next Review Date:	28/02/2021
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	01/04/2014
Counties Manukau District Health Board			

released under Official Information Act - ref OIA 2016-2020 Wey Lovatt

	<p><i>Types of harm for CM Health:</i></p> <ul style="list-style-type: none"> • Loss of trust • Loss of assets • Financial exposure, e.g. fines and penalties • Legal proceedings <p><i>Types of harm for the public:</i></p> <ul style="list-style-type: none"> • Risk to public health • Risk to public safety <hr/> <p>Is the information in the hands of people whose intentions are unknown or possibly malicious?</p> <p>For example, was the information taken by or given to an unknown recipient or one suspected of illegal activity? Was the recipient a trusted, known person or organisation that could be expected to return the information?</p>
--	--

STEP 3: Notify affected people if necessary

<p>Being open and transparent with individuals about how personal information is being handled is a fundamental rule of privacy.</p>	<p>Notification can be a key step to help individuals affected by the breach and show that CM Health is doing the right thing. If a breach creates a risk of harm to the individual, those affected should usually be notified. Prompt notification can help lessen the damage by taking steps to protect themselves and regain control of that information.</p> <p>But do not notify people unless you are sure of the people whose information has been compromised by the breach. More damage can be done if the wrong people are notified in error.</p> <p>When to notify</p> <p>It is not always necessary to notify breaches if there is no risk of harm, notification can be overkill and on occasion, notification can do more harm than good. Each incident needs to be considered on a case-by-case basis. CM Health will also inform the Office of the Privacy Commissioner of material privacy breaches so that it is also aware of the breach and can handle any related enquiries or complaints.</p> <p>Consider:</p> <ul style="list-style-type: none"> • What is the risk of harm to people whose information has been breached? • Is there a risk of identity theft or fraud?
--	---

Document ID:	A321063	CMH Revision No:	2.0
Division:	Executive Management	Last Review Date :	1/03/2018
Document Owner:	Risk and Privacy Manager -Strategic Development	Next Review Date:	28/02/2021
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	01/04/2014
Counties Manukau District Health Board			

	<ul style="list-style-type: none"> • Is there a risk of physical harm? • Is there a risk of humiliation or loss of dignity, damage to the individual’s reputation or relationships, for example when the information lost includes mental health, medical or disciplinary records? • What is the person’s ability to avoid or minimise possible harm? • What are the legal and contractual obligations? <p>By now, you should have as complete a set of facts as possible and completed your risk assessment in order to determine whether to notify individuals. Notification should occur as soon as reasonably possible. But if law enforcement authorities are involved, check with those authorities on when to notify so that their investigation is not compromised.</p>
	<p>How to notify</p> <p>It is always best to notify affected individuals directly – by phone, letter, and email or in person. Direct notification is more sincere and personal. Indirect notification – website information, posted notices, media – should generally occur where direct notification could cause further harm, is prohibitively costly or the contact information is not known. Using multiple methods of notification may also be appropriate. It is also important to consider whether notification might reveal the value of the missing information. For particularly vulnerable people, consider notifying them through or with a support person.</p>
	<p>Who should notify</p> <p>Notification to individuals affected by a breach should generally come from the service in which the breach has occurred however there will be situations where it will be more appropriate for the service which has the most significant relationship with the individual to notify them. Where there has been a serious breach, notification may need to come from the relevant General Manager, Chief Operating Officer or the Chief Executive Officer.</p> <p>This will be determined by the Risk and Privacy Manager, in consultation with Legal as appropriate.</p>
	<p>What to say</p> <p>Breach notification should generally contain:</p> <ul style="list-style-type: none"> • Information about the incident, including when it happened • A description of the personal information that has been

Document ID:	A321063	CMH Revision No:	2.0
Division:	Executive Management	Last Review Date :	1/03/2018
Document Owner:	Risk and Privacy Manager -Strategic Development	Next Review Date:	28/02/2021
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	01/04/2014
Counties Manukau District Health Board			

released under Official Information Act 1982 / OIA 25062020 Van May Lovatt

	<p>disclosed and what has not been disclosed</p> <ul style="list-style-type: none"> • What CM Health is doing to control or reduce the harm • What CM Health is doing to help people and what steps they can take to protect themselves • Contact information for enquiries and complaints • Offers of assistance when necessary • Whether CM Health has notified the Office of the Privacy Commissioner • Information about the individual’s right to complain to the Privacy Commissioner and contact information for the Privacy Commissioner. <p>A letter of apology should follow notification as this provides written confirmation of the breach, actions taken to reduce harm or mitigate the risk, process improvements to prevent future harm and the contact details of the Office of the Privacy Commissioner should they wish to lodge a complaint.</p> <p>Refer to Appendix D for Notification/ Apology template.</p>
	<p>Notifying third parties</p> <p>Consider whether any of the following groups of organisations should also be informed:</p> <ul style="list-style-type: none"> • Office of the Privacy Commissioner • healthAlliance – for IT related incidents for example – notifying them on the theft of computers • Other District Health Board, particularly those in the Northern Region • Police • Insurers • Professional or other regulatory bodies • Third party contractors or other parties who might be affected • Internal business units not previously advised of the privacy breach for example Communications, Legal, other members of senior management • The Board and the Ministry of Health • Union or other employee representatives <p>One agency that should be notified of any serious breaches is the Office of the Privacy Commissioner. This will help the Privacy Commissioner respond to inquiries made by the public and to complaints that might be received. The Privacy Commissioner may also be able to provide advice or guidance to your agency that may be helpful in responding to the breach. Notification helps to show</p>

Document ID:	A321063	CMH Revision No:	2.0
Division:	Executive Management	Last Review Date :	1/03/2018
Document Owner:	Risk and Privacy Manager -Strategic Development	Next Review Date:	28/02/2021
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	01/04/2014
Counties Manukau District Health Board			

	<p>that CM Health is being responsible and taking the matter seriously. All communication/ notification to the Office of the Privacy Commissioner will be through the Risk and Privacy Manager.</p>
--	---

STEP 4: Prevent a repeat

	<p>Do not assume that there is nothing that can be fixed or done to prevent future mistakes. There's a system failure behind many errors and now is a good opportunity to learn from the mistake. There are a number of steps CM Health can take to minimise or prevent breaches.</p> <p>After a breach, CM Health needs to take the time to investigate the cause of the breach and make changes to the prevention plan and how it is being applied. This may require corrective actions to be formalised and implemented.</p> <p>The amount of effort should reflect the significance of the breach, and whether it happened as a result of a systemic problem or an isolated event. It could include:</p> <ul style="list-style-type: none"> • A security audit of both physical and technical security • A review of policies and procedures • A review of employee training practices • A review of any service delivery partners caught up in the breach <p>The resulting corrective action plan should be assessed by the service manager to ensure the adequacy and effectiveness of the mitigation.</p>
--	--

released under Official Information Act ref: OIA 23062020 Valley Lovatt

Document ID:	A321063	CMH Revision No:	2.0
Division:	Executive Management	Last Review Date :	1/03/2018
Document Owner:	Risk and Privacy Manager -Strategic Development	Next Review Date:	28/02/2021
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	01/04/2014
Counties Manukau District Health Board			

Appendix B – Reporting and Escalation Matrix

Criteria	Detail	Rating	Scoring
Number of individual affected	Single individual	10	
	2-10 individuals	20	
	11-50 individuals	40	
	51 or more individuals	60	
Sensitivity of the information (select the highest level of sensitivity involved)	Minor sensitivity (e.g. name, employment position)	10	
	More sensitivity (e.g. remuneration, contact details)	20	
	Sensitive (e.g. financial, biometric)	50	
	Highly sensitive (e.g. health, criminal records, information about people at risk, closed records, contact details for vulnerable people)	80	
Potential or actual harm to individual(s) You can select several types of harm potential and/ or actual harm. If an actual harm occurred, do not select the corresponding potential harm.)	No potential or actual harm to the individual(s)	0	
	Potential for financial loss to the individual(s)	20	
	Potential for identity theft	25	
	Actual unwarranted intrusion into the individual's personal life	20	
	Potential for loss of business, employment or other opportunities for the individual(s)	25	
	Potential for hurt, humiliation or reputational damage to the individual(s)	30	
	Individual denied access to, correction of or statement of correction not included with their information without good reason	30	
	Actual financial loss to the individual(s)	40	
	Potential for physical harm to the individual(s)	50	
	Actual identity theft	50	
	Actual loss of business, employment or other opportunities for the individual(s)	50	
	Actual hurt, humiliation or reputational damage to the individual(s)	60	
	Actual physical harm to the individual(s)	100	
Potential or	No potential or actual harm to CM Health	0	

Document ID:	A321063	CMH Revision No:	2.0
Division:	Executive Management	Last Review Date :	1/03/2018
Document Owner:	Risk and Privacy Manager -Strategic Development	Next Review Date:	28/02/2021
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	01/04/2014
Counties Manukau District Health Board			

Criteria	Detail	Rating	Scoring
actual harm to CM Health	Potential for loss of business opportunity for CM Health	10	
	Potential for financial loss to CM Health	20	
	Potential for reputational damage to CM Health	20	
	Potential for loss of trust in CM Health or wider public sector	20	
	Loss of business opportunity for CM Health	20	
	Financial loss to CM Health	40	
	Reputational damage to CM Health	40	
	Loss of trust in CM Health or wider public sector	40	
	More than one type of harm to CM Health	50	
Potential for media attention	No media interest occurring or likely to occur	0	
	Some media interest occurring or likely to occur	20	
	Widespread media interest occurring or likely to occur, and CM Health, GCPO, OPC and others may be asked to comment	50	
Privacy breach source	Inadvertent information handling error (e.g. email or letter sent to incorrect recipient, information provided to the wrong person over the telephone.	10	
	Patient lists/ file left in an unsecure location (lost/ misplaced)	20	
	Information used by CM Health for a purpose not related to collection, and an exception does not apply	20	
	Failure to provide access to personal information within statutory or extended timeframe, or failure to correct or attach a statement of correction to personal information	30	
	Theft or loss of property containing personal information (e.g. USB stick, documents, laptop or other such mobile device)	40	
	Information collected by unlawful, unfair or unreasonably intrusive means	50	
	Unauthorised access of systems or information (e.g. staff member accessing information not for work purposes and contrary to agency policies/ procedures.	50	
	Systemic system or business process issue (e.g. insufficient security controls, asking for and receiving information not necessary for purpose, not responding to requests, withholding information	60	

Document ID:	A321063	CMH Revision No:	2.0
Division:	Executive Management	Last Review Date :	1/03/2018
Document Owner:	Risk and Privacy Manager -Strategic Development	Next Review Date:	28/02/2021
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	01/04/2014
Counties Manukau District Health Board			

Criteria	Detail	Rating	Scoring
	without good reason, retaining information received through an information matching programme)		
	Cyber security incident (e.g. hacking)	60	
Status of the privacy breach	Information recovered, destroyed and not access by an unauthorised individual	1	
	Individual provided access to their information, or information corrected/ statement of correction included	10	
	Information not recovered but encrypted and unlikely to be accessible	20	
	Information recovered/ destroyed/ no physical copy disclosed, and accessed by an unauthorised individual(s)	50	
	Systemic or business process issue fixed, but information was accessed by an unauthorised individual(s)	50	
	Information not recovered and accessible	60	

released under Official Information Act - ref OIA 23062020 Van Wey Lovatt

Document ID:	A321063	CMH Revision No:	2.0
Division:	Executive Management	Last Review Date :	1/03/2018
Document Owner:	Risk and Privacy Manager -Strategic Development	Next Review Date:	28/02/2021
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	01/04/2014
Counties Manukau District Health Board			

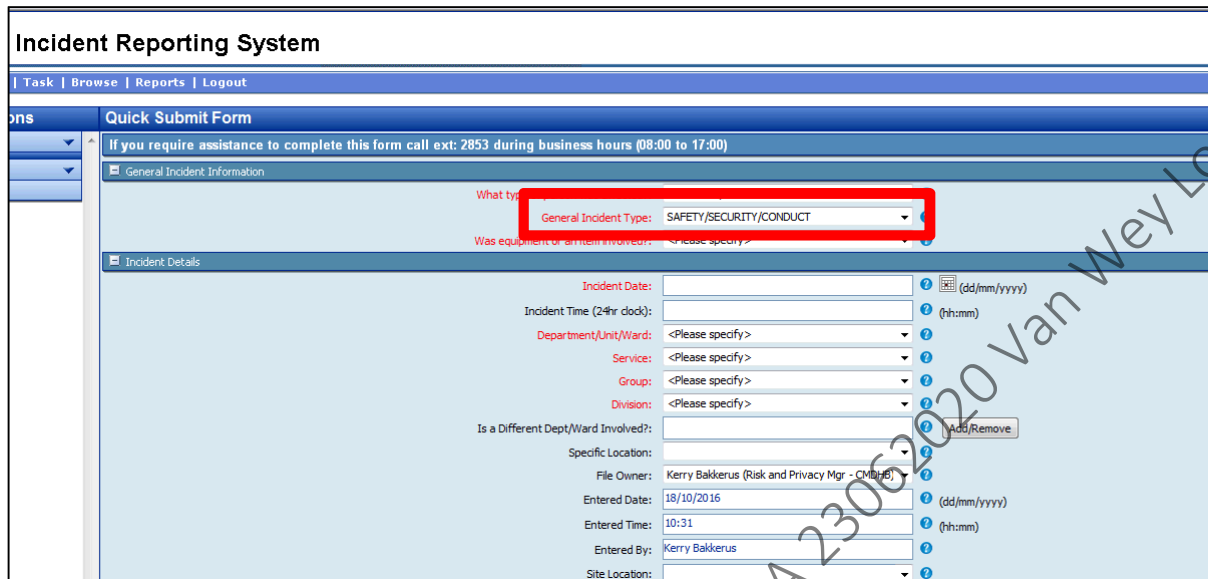
PRIVACY BREACH IMPACT RATINGS

Rating range	Level	Descriptor	Escalation and Reporting
0-170	5	<p>Small number of people affected, with little or no potential or actual harm to the individual(s).</p> <p>Little or no indication of systemic problems within CM Health.</p>	Privacy Officer and Legal
171-220	4	<p>Small number of people affected, with minor potential or actual harm to the individual(s).</p> <p>Little or no indication of systemic problems within CM Health.</p>	
221-270	3	<p>Either the information is not sensitive/ highly sensitive and the potential or actual harm to the individual(s) is more than minor, or the information is sensitive/ highly sensitive and the potential or actual harm to the individual(s) is minor.</p> <p>Individuals may stop using, or be reluctant to use a service. The incident may get media attention or cause reputational risk.</p>	As with 4-5 rating, including: Clinical Governance Group (c/o Chief Medical Officer), Communications Team and CEO
271-320	2	<p>Breach of sensitive or highly sensitive information, with serious potential or actual harm to the individual(s).</p> <p>The incident may imply a systemic failure that could undermine agency systems. The incident may cause long term loss of trust and confidence in CM Health that could impact service delivery. There could be measurable and on-going negative impact on individuals and/or agencies. On-going media coverage.</p>	As with 3-5 rating, including: Audit, Risk and Finance Committee with communication to the CEO and Chair.
321 and above		<p>Breach of sensitive or highly sensitive information, with serious potential or actual harm to the individual(s). It is likely that more than one type of harm has occurred, and that harm is likely to be on-going.</p> <p>There may be a systemic failure that could undermine CM Health's systems. If public, will significantly affect the reputation of and trust and confidence in the State Sector. On-going media coverage.</p>	

Document ID:	A321063	CMH Revision No:	2.0
Division:	Executive Management	Last Review Date :	1/03/2018
Document Owner:	Risk and Privacy Manager -Strategic Development	Next Review Date:	28/02/2021
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	01/04/2014
Counties Manukau District Health Board			

Appendix C - Guideline for logging a breach within the Incident Management System

- All incidents need to be logged into the system - [Incident Management System - login here.](#)
- In the 'General Incident Type' select 'Safety/ Security/ Conduct'.



The screenshot shows the 'Incident Reporting System' interface. At the top, there is a navigation bar with 'Task | Browse | Reports | Logout'. Below this is a 'Quick Submit Form' section with a note: 'If you require assistance to complete this form call ext: 2853 during business hours (08:00 to 17:00)'. The main form area is divided into 'General Incident Information' and 'Incident Details'. In the 'General Incident Information' section, the 'General Incident Type' dropdown menu is highlighted with a red box and contains the text 'SAFETY/SECURITY/CONDUCT'. Other fields include 'Incident Date', 'Incident Time (24hr clock)', 'Department/Unit/Ward', 'Service', 'Group', 'Division', 'Is a Different Dept/Ward Involved?', 'Specific Location', 'File Owner', 'Entered Date', 'Entered Time', 'Entered By', and 'Site Location'.

- In the 'Specific Incident Type' select 'Breach of Privacy'.

released under Official Information Act - ref OIA 23062020 Van Wey Lovatt

Document ID:	A321063	CMH Revision No:	2.0
Division:	Executive Management	Last Review Date :	1/03/2018
Document Owner:	Risk and Privacy Manager -Strategic Development	Next Review Date:	28/02/2021
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	01/04/2014
Counties Manukau District Health Board			

ent Form - Windows Internet Explorer
 http://mmhincrp01/rmproweb/Riskweb3.dll/FrmIncQuickEntry

View Favorites Tools Help

Online Incident Form Privacy, Security and Trust.

Incident Reporting System

Task | Browse | Reports | Logout

Quick Submit Form

Specific Location: [Dropdown]
 File Owner: Kerry Bakkerus (Risk and Privacy Mgr - CMDHB)
 Entered Date: 18/10/2016 (dd/mm/yyyy)
 Entered Time: 10:31 (hh:mm)
 Entered By: Kerry Bakkerus
 Site Location: [Dropdown]

Name	Phone	Reported Date	Time
Kerry Bakkerus		18/10/2016	10:31

Witnesses [Add]

People Involved Name	People Involved Phone
(No Data)	

Specific Incident Details

Specific Incident Type: **breach of privacy**

Is this a OHSO Hazard and safety issue? <Please specify>

Immediate Actions Taken: [Text] [Add/Remove]

Contributing Factors: [Text] [Add/Remove]

Reported Incident Severity: <Please specify>

Actual Incident Severity: <Please specify>

Short Description of Events (NO NAMES): [Text] [Add/Edit]

released under Official Information Act - ref OIA 23062020 Van Wey Lovatt

Document ID:	A321063	CMH Revision No:	2.0
Division:	Executive Management	Last Review Date :	1/03/2018
Document Owner:	Risk and Privacy Manager -Strategic Development	Next Review Date:	28/02/2021
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	01/04/2014
Counties Manukau District Health Board			

Appendix D – Notification Template



Private Bag 93311
Otahuhu 1640
Auckland, New Zealand
Telephone 64-9-276-0000

(Insert date here)

Private & Confidential

(Insert addressee)

Insert address [physical/ email]

Dear Addressee

Breach of Privacy

- Information about the incident, including when it happened
- A description of the personal information that has been disclosed and what has not been disclosed
- What CM Health is going to control or reduce the harm
- What CM Health is doing to help people and what steps they can take to protect themselves
- Contact information for enquiries and complaints
- Offers of assistance when necessary
- Whether CM Health has notified the Office of the Privacy Commissioner
- Information about the individual's right to complain to the Privacy Commissioner and contact information for the Privacy Commissioner.

We want you to know that privacy is taken very seriously at Counties Manukau Health and that this inadvertent incident has been an unfortunate aberration which we will take the greatest care not to repeat. We sincerely apologise for any distress caused to you. Please contact me if you would like to meet, or if there is any further information or assistance that we can provide.

You have the right to raise a complaint with the Office of the Privacy Commissioner, through the following options:

- Lodge your complaint online (<https://www.privacy.org.nz/your-rights/complaint-form/>)
- Download the complaint form to complete, then:
 - Mail: Office of the Privacy Commissioner, PO Box 10094, Wellington 6143
 - Fax: 04 474 7595
 - Email: enquiries@privacy.org.nz

Document ID:	A321063	CMH Revision No:	2.0
Division:	Executive Management	Last Review Date :	1/03/2018
Document Owner:	Risk and Privacy Manager -Strategic Development	Next Review Date:	28/02/2021
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	01/04/2014
Counties Manukau District Health Board			

Yours faithfully

Insert name

Title

Counties Manukau Health

released under Official Information Act - ref OIA 23062020 Van Wey Lovatt

Document ID:	A321063	CMH Revision No:	2.0
Division:	Executive Management	Last Review Date :	1/03/2018
Document Owner:	Risk and Privacy Manager -Strategic Development	Next Review Date:	28/02/2021
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	01/04/2014
Counties Manukau District Health Board			

Procedure: Storage and Security of Electronic and Paper Clinical Records

Abstract

Reasonable safeguards should be put in place to protect personal information against loss, misuse, or unauthorised access, use, modification or disclosure. This procedure outlines the processes that staff should follow to ensure the security of the electronic and paper clinical records at all times.

Procedure:

Physical Security of Paper Clinical Records:

The health information must be protected while in use, storage or in transit.

Security of Clinical Records when they are stored in locations other than the Clinical Records Department:

The person receiving the paper clinical record(s) is responsible for the security of the record while they are stored in locations other than the Clinical Records Department.

Example:

Ward clerks who receive the paper clinical records into the Ward and up-date the iPMS Tracking System are responsible for the security of the record whilst it is on the ward.

Patient Care Assistants who receive the clinical records at the Superclinic are responsible for the security of the record whilst it is in the Module.

Those clinical records which are stored in areas that only allow staff “swipe card” access or that cannot be accessed by the public when left unattended do not have to be locked away.

However, those clinical records which are held in areas where they could be accessed by the public when left unattended must be locked away to minimise the risk of unauthorised access.



Important: All requests for copies of clinical records from other health care providers must be processed through the Clinical Records Department. CM Health staff, who receive such requests directly, must refer the requester to the Clinical Records Department.

Document ID:	A7366	CMH Revision No.:	1.2
Service :	N/A - Controlled document used across the organisation	Last Updated:	27/03/2019
Document Owner:	Risk and Privacy Manager - Strategy and Infrastructure	Next Review Date:	27/03/2021
Approved By:	Health Information Committee (HIC)	Date First Issued:	1 March 2004

If you are not reading this document directly from the Document Directory this may not be the most current version



Important: Staff must not remove clinical records from any of the CM Health premises without authorisation from the Clinical Records Dept or staff responsible for the clinical records in outlying units. If authorisation to remove clinical records from the CM Health premises has been obtained, the records must be kept secure eg in a locked bag or case. It is not appropriate to leave clinical records in an unattended car, even if that car is locked, as that is not sufficiently secure. Clinical staff working in the community are an exception and if they do need to leave clinical records in the car, they should be locked in the car boot and not visible to passers by.

All third party requests for health information held in electronic or paper clinical records must be referred to the Release of Information Officer in the Clinical Records Department. Staff who receive such requests directly must refer the requester to the Clinical Records Department.

Tracking the Location of the Paper Clinical Records:

To ensure that the location of the paper record is known at all times, the following information will be tracked using the iPMS Tracking System:

- Name of person who has requested or is using the clinical records
- Reason for Use (eg audit, “to view”)
- Normal storage location of the records
- The current location of the records
- Date of dispatch
- Date of receipt



Important: Staff who dispatch the records to another location are responsible for up-dating iPMS Tracking System.
Those staff who receive the records are responsible for up-dating the iPMS Tracking System.

Operational Security:

Who may Access the Clinical Record:

Staff of CM Health, authorised students accommodated within CM Health, and staff of approved health providers associated with CM Health may access the clinical records (including the electronic record) of patients for whom they are providing ongoing care and treatment. This includes administrative tasks such as booking patients for appointments etc.

Document ID:	A7366	CMH Revision No.:	1.2
Service :	N/A - Controlled document used across the organisation	Last Updated:	27/03/2019
Document Owner:	Risk and Privacy Manager - Strategy and Infrastructure	Next Review Date:	27/03/2021
Approved By:	Health Information Committee (HIC)	Date First Issued:	1 March 2004

If you are not reading this document directly from the Document Directory this may not be the most current version

Procedure: (continued)

Records must not be accessed or used other than for an authorised purpose related to the care and treatment of patients under the staff member's care in that staff member's role at CM Health.

Confidentiality:

The "misuse of confidential information, failure to respect the confidentiality of patient information" is not permitted and is defined in the CM Health [Code of Conduct](#) as serious misconduct.

Each employee is required to sign an Employee Confidentiality Agreement on commencement of employment.



Warning: All incidents of failure to respect patient confidentiality are considered to be serious misconduct, and may result in disciplinary action which may include dismissal.

Many staff have ready access to all patients' health information via the electronic records such as Concerto and PiMS. Obtaining access to this information to provide ongoing care and treatment, or for administrative purposes is acceptable use of the information. However, staff may not look up their own results, appointments, referrals etc on the electronic or paper record without following the procedures outlined in "[How Patients Gain Access to their own Personal Health Information](#)".

Staff may use other accepted methods of obtaining this information, for example, telephoning "Inquiries" or the Manukau Superclinic Call Centre.

Staff must never look up the results or health information of their relatives or friends. Access to information about family members or friends can only be obtained by following the procedures outlined in "[How Relatives/Friends Obtain Personal Health Information about a Patient](#)".

Document ID:	A7366	CMH Revision No.:	1.2
Service :	N/A - Controlled document used across the organisation	Last Updated:	27/03/2019
Document Owner:	Risk and Privacy Manager - Strategy and Infrastructure	Next Review Date:	27/03/2021
Approved By:	Health Information Committee (HIC)	Date First Issued:	1 March 2004
<i>If you are not reading this document directly from the Document Directory this may not be the most current version</i>			

Procedure: (continued)

Warning: It is considered misuse and unauthorised access if staff look up their own or family members/friends results, appointments, referrals etc on the electronic or paper clinical record. The usual processes must be followed: for access to a staff member's own information, he/she must follow the "How patients gain access to their own personal health information" procedure, and for access to a family member or friend's information, the staff member must follow the "How Relatives/Friends obtain Personal Health Information about a Patient" procedure.

Staff should avoid collecting health information from patients in public waiting areas where members of the public or unauthorised personnel could overhear the discussion.

Health information must be made anonymous for health education purposes, eg for Grand Round presentations, and fictitious information should be used when training staff to use the systems.

Technical Security:**Use of Passwords for Electronic Clinical Records:**

The security of passwords or electronic identifier is the responsibility of the individual staff member. All authorised staff will be held responsible for any use of their electronic identity and signature. Any security breach or compromise of an electronic identifier must be reported immediately.

All users should use a "strong" password that cannot be easily guessed or identified. Never use names of family members, pets, birth dates or common or generic passwords such as "password" or "letmein". Strong passwords should be at least 7 characters long and should have a combination of letters and numbers.



Warning: It is not a defence against performance management proceedings, that an individual's password was known to others. All notified security breaches of electronic health information will be performance managed.

Document ID:	A7366	CMH Revision No.:	1.2
Service :	N/A - Controlled document used across the organisation	Last Updated:	27/03/2019
Document Owner:	Risk and Privacy Manager - Strategy and Infrastructure	Next Review Date:	27/03/2021
Approved By:	Health Information Committee (HIC)	Date First Issued:	1 March 2004

If you are not reading this document directly from the Document Directory this may not be the most current version



Warning: Health information about patients must not be sent electronically to external health care providers unless a secure e-mail system is in place or the document is protected by secure password.

Related Documents:

NZ Legislation	Privacy Act 1993 Health Information Privacy Code 1994 Official Information Act 1982 Health Act 1956 Public Records Act 2005
CMDHB Clinical Board Policies and Procedures	03 Sharing Health Information with Providers of Care 04 Documentation in the Clinical Record 05 Storage and Security of Clinical Records 06 How Patients Access Their Own Information 07 How Parents and Guardians Request Personal Health Information 08 Altering Personal Health Information at the Patient's Request 09 Checking for accuracy and authorising entries into the clinical record 10 Correcting inaccuracies in the clinical record 11 Disclosing Anonymous Health Information 12 Employee Initiated Unanticipated Disclosure 13 Third Party requests 14 Disclosure of Health Information to Relatives, Friends Inpatient coding through the discharge summary Release of Information from Decision Support Services Retention and Destruction of Personal Health Information
Quality Health NZ Standards	Information Management (Acute Care, 2001, Version 2)
Other CMDHB Policies and Procedures	HR Policies – Code of Conduct IS Policies – Security of Information on Computer Equipment
Other related documents	Southnet – Privacy and Legal Intranet site.

Document ID:	A7366	CMH Revision No.:	1.2
Service :	N/A - Controlled document used across the organisation	Last Updated:	27/03/2019
Document Owner:	Risk and Privacy Manager - Strategy and Infrastructure	Next Review Date:	27/03/2021
Approved By:	Health Information Committee (HIC)	Date First Issued:	1 March 2004

If you are not reading this document directly from the Document Directory this may not be the most current version

Procedure: Sharing Health Information with Providers of Health Care Services to CM Health Patients -

Purpose

One of the purposes for collecting personal health information from patients, and using it, is to provide ongoing care and treatment. This includes sharing relevant health information with other providers of health care services who are involved in the patient's treatment. When a patient is referred to CM Health by a General Practitioner (GP), midwife or other provider of health services, it is important that the outcome of the referral is documented in the patient's clinical record and communicated back to the referrer.

This procedure outlines the processes that staff should follow to ensure health information is appropriately shared with general practitioners, mid-wives and other health care providers who have referred patients for treatment at CM Health or are involved in the patient's treatment.

Procedure



Important: Patients should be made aware that their health information will be shared with other health professionals who are providing ongoing care and treatment, including their GP.

Sharing of Health Information for In-patients:



Important: Disclosing patient information to the patient's GP or other health care provider is permitted, as sharing information with other health care professionals is one of the purposes for which it is collected.

Electronic Discharge Summary:

- An Electronic Discharge Summary (EDS) must be completed on the day a patient is discharged from hospital, a copy of the EDS must be sent to the referring health care provider, eg GP, midwife etc.
- If the referrer is not the patient's usual GP, a copy should be sent to the usual GP, unless the patient specifically asks that his/her usual GP not receive the information.
- If early, post-discharge monitoring by the referrer is required, the health care provider should telephone the referrer prior to sending out the EDS, so that formal transfer of responsibility is established at that point.

Document ID:	A7365	CMH Revision No:	1.2
Service:	Clinical Governance	Last Review Date :	15/04/2019
Document Owner:	Patient Information Service Manager	Next Review Date:	15/04/2022
Approved by:	Health Information Committee (HIC)	Date First Issued:	03/03/2004

If you are not reading this document directly from the Document Directory this may not be the most current version.

Other In-patient Documentation:

Other types of health information which are collected during a patient's in-patient stay which may be shared with other health care providers include:

- Operation notes
- Ward round notes
- Ward reviews
- Ward referrals
- Test results and x-ray reports.

Copies of the above reports will be sent to the GP at the request of the author, who must dictate these instructions to the transcriptionist.

Sharing Health Information for Out-patients:

All GPs, mid-wives etc who refer patients for outpatient treatment must receive information about their patients from CM Health clinicians, in the form of dictated/typed letters or reports:

- Clinic letters or reports dictated immediately after each outpatient visit, including on discharge from the clinic.
- Clinic letters or reports dictated immediately after each outpatient procedure
- Result letters, if significant results are returned after the clinic which the GP needs to be made aware of
- Administration letters dictated if significant changes in management are required between out-patient visits
- If the referrer is not the patient's usual GP, a copy should be sent to the usual GP, unless the patient specifically asks that his/her usual GP not receive the information.

Related Documents:

NZ Legislation	Privacy Act 1993
	Health Information Privacy Code 1994
	Official Information Act 1982
	Health Act 1956
	Archives Act 1952

Document ID:	A7365	CMH Revision No:	1.2
Service:	Clinical Governance	Last Review Date :	15/04/2019
Document Owner:	Patient Information Service Manager	Next Review Date:	15/04/2022
Approved by:	Health Information Committee (HIC)	Date First Issued:	03/03/2004

If you are not reading this document directly from the Document Directory this may not be the most current version.

Sharing Health Information with Providers of Health Care Services to CM Health Patients -

CMDHB Clinical Board Policies and Procedures	Correcting & Altering Personal Health Information at the Patient's Request - Procedure Checking for accuracy and authorising entries into the clinical record Procedure Correcting inaccuracies in the clinical record Procedure Disclosing Anonymous Health Information Procedure Documentation in the Clinical Record - Procedure Disclosure of Health Information to Relatives, Friends Procedure Employee Initiated Unanticipated Disclosure Procedure How Parents and Guardians Request Personal Health Information Procedure How Patients Access Their Own Information Procedure Inpatient Coding through the Discharge Summary Procedure Release of Information from Decision Support Services Policy Retention and Destruction of Personal Health Information Policy Safe Management and Privacy of Personal Health Information Policy Storage and Security of Clinical Records Third Party Requests Procedure
Quality Health NZ Standards	Information Management (Acute Care, 2001, Version 2)
Other CMDHB Policies and Procedures	HR Policies – Code of Conduct IS Policies – Security of Information on Computer Equipment
Other related documents	SouthNET Privacy and Legal Intranet site.

Document ID:	A7365	CMH Revision No:	1.2
Service:	Clinical Governance	Last Review Date :	15/04/2019
Document Owner:	Patient Information Service Manager	Next Review Date:	15/04/2022
Approved by:	Health Information Committee (HIC)	Date First Issued:	03/03/2004

If you are not reading this document directly from the Document Directory this may not be the most current version.

Policy: Clinical Audit

Purpose

Counties Manukau Health is committed to improving the quality of services being offered to users. Clinical audit is an important activity because it provides findings which demonstrate whether or not the organisation is practicing effectively.

The purpose of this policy is to outline how audits should be co-ordinated, monitored and evaluated; it also aims to ensure that authorisation processes are robust, and that duplication is minimised.



Note: This policy must be read in conjunction with relevant CMDHB audit Procedures and Guidelines.

Scope

This policy applies to clinical audits performed by Counties Manukau Health (CM Health) staff. This includes audit activities where CM Health staff members are subjects of the audit. As audits may vary substantially in scale and implications, some judgement must be exercised in considering which audits require registration – for example, audits which review and have implications only for the practice of an individual clinician who is undertaking an audit of their own practice for individual professional development purposes need not be registered, whereas audits which review and have implications for future service provided by a team should generally be registered to support ongoing organisational learning and quality assurance. Advice on this point should be sought from the relevant Clinical Leader, Service Manager or a member of the Research Office if required.

Policy

Governance

The CM Health Research Committee (RC) is responsible for ensuring adherence to the policy for audits conducted at CM Health or on behalf of CM Health. The RC is a subcommittee of the CM Health Clinical Governance Group.

The CM Health Research Office (CM Health RO) is responsible for registering audit activities where this is requested. The research office further ensures that all audit activities have the necessary approvals in place and comply with CM Health policies, as well as any appropriate external regulatory and approval requirements.

CMDHB Approval

Audits should have a clearly defined purpose that is useful in improving clinical practice and that is in line with organisational priorities. Audit projects should not result in duplication of effort. The impact of an audit on the service's ability to perform its operations should be clearly identified.

Any clinical audit carried out within CM Health facilities must be facilitated by a CM Health clinician. Patient/client rights with regards to privacy should be safeguarded with appropriate authorisation for release of patient information.

Costs of carrying out the audit should be accurately identified and should not overburden CM Health resources. There is a balance between resources used, and the expected outcomes of the audit.

Clinical auditors who register audits with the Research Office should discuss audit proposals with the relevant **Clinical Leader** and **Service Manager**, and prior to

Document ID:	A11138	CMH Revision No:	3.0
Service :	N/A - Controlled document used across the organisation	Last Review Date :	1/04/2019
Document Owner:	Research Officer - Health Intelligence and Informatics	Next Review Date:	1/04/2022
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	21/05/2010
<i>If you are not reading this document directly from the Document Directory this may not be the most current version.</i>			

Audit Policy

commencing obtain formal approval from them.

All audits registered with the CM Health Research Office may be audited by the RC or a person appointed by the RC to ensure compliance with this policy.

Registration with the CMH Research Office All audits must be registered with the Research Office to obtain a registration number. Registration should occur after the feasibility of the proposed audit has been discussed with the relevant Clinical Leader and Service Manager.

Ethical Review Audit activity does not require ethics committee review, unless it reaches a threshold of more-than-minimal risk (refer to procedures). Ethics committee review may be beneficial if the audit is intended for publication.

Requirements for Non-CMDHB Research Partners Where the Coordinating Investigator is a non-CMDHB auditor and the audit team does not include a CMDHB employee, an audit Facilitator must be identified. If an appropriate audit facilitator has not been identified and confirmed, the relevant Manager is responsible for appointing a CMDHB employee as an audit facilitator. Audit Facilitators are responsible for ensuring the audit meets CMDHB requirements.

All non-CMDHB staff involved in CMDHB audit must sign a confidentiality agreement and submit this to the RO before the audit commences. A separate confidentiality agreement must be signed for each new audit study.

Study Conduct All audits conducted at CMDHB must:

- Be conducted according to the highest ethical and scientific standards and comply with the appropriate local, national, and international guidelines and processes.
- Respect and protect the rights and well being of the participants involved in audit, as specified in the Code of Health and Disability Services Consumers' Rights (1996).
- Have appropriate approvals (clinical leader and service manager or delegated managers for registration with the RO).
- Ensure that the audit data and records are accurate, complete, securely stored for the relevant retention period and will be available for future review or audit by internal or external parties.
- Comply with all other relevant CMDHB Policies, Procedures and Guidelines.

All adverse events occurring in audit conducted at CMDHB must be reviewed by the Coordinating Investigator who is required to:

- Make a decision based on the level of risk and potential harm and take appropriate actions to protect all patients and auditors;
- Meet the regulatory HDEC and SCOTT reporting requirements;
- Report all suspected unexpected serious adverse reactions (SUSAR) to the Research Committee; and
- Report all adverse events that meet the criteria for CMDHB Incident Reporting.

Resource Usage The resources associated with audit involving CMDHB must be clearly identified by the auditor.

Document ID:	A11138	CMH Revision No:	3.0
Service :	N/A - Controlled document used across the organisation	Last Review Date :	1/04/2019
Document Owner:	Research Officer - Health Intelligence and Informatics	Next Review Date:	1/04/2022
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	21/05/2010
<i>If you are not reading this document directly from the Document Directory this may not be the most current version.</i>			

Audit Policy

Where the resource usage relates to a cost incurred (including use of a service), this cost must be covered. Where a CMDHB Department is willing to cover the costs associated with the audit, this must be approved by the relevant manager or an appropriate delegate. Where resource usage relates to use of staff time, this must be approved by the appropriate Manager.

Treaty of Waitangi Consultation of and All audit involving CMDHB must be consistent with the provisions of the Treaty of Waitangi and as such meets the rights, needs and interests of Maaori.

Other Cultural Consultation It is the responsibility of the Coordinating Investigator to ensure that any other cultural consultation appropriate to their audit is undertaken if required.

Fraud or Misconduct audit in All CMDHB employees involved in auditing are required to report any case of suspected audit Fraud / Misconduct in line with CMDHB policies on Just Culture (v1 15 Feb 2010) and Fraud Monitoring and Management (v1 July 2007).

Definitions

A clinical audit asks 'are we following best practice?' and 'what is happening to patients as a result'. Audit is a measurement of current practice against an agreed standard. Audit does not seek to establish or define what best practice is. It does NOT involve new treatment/practice, nor control groups or placebo groups, or allocating patients to different treatment groups.

"Research is concerned with discovering the right thing to do; audit with ensuring that it is done right." *Smith, R. Audit & Research. BMJ 1992; 305: 905-6*

"Research is about obtaining new knowledge and finding out what treatments are the most effective. Clinical audit is about quality and finding out if best practice is being practised. Research tells us what we should be doing. Clinical audit tells us whether we are doing what we should be doing and how well we are doing it."
Healthcare Quality Improvement Partnership, UK, 2012

"Audit is the process of reviewing the delivery of health care to identify deficiencies so that they may be remedied." *K. Crombie 1997*

"The systematic peer evaluation of an aspect of patient care. The process, which may be multidisciplinary, involves a cycle of continuous improvement of care based on explicit and measurable indicators of quality. These indicators include a service user perspective...The principle of all clinical audit activity is that it leads to improvements in clinical practice, resulting in improved outcomes for patients."
Ministry of Health Working Party; Towards Clinical Excellence – An Introduction to Clinical Audit, Peer Review and Other Clinical Practice Improvement Activities 2002

"Clinical audit is the quantitative assessment of the quality of care being provided compared to agreed, documented evidence-based criteria or to the performance of other providers...Its aim is both to stimulate quality improvement interventions and to assess their impact." *U.K. National Clinical audit Advisory Group, Department of Health 2009*

Document ID:	A11138	CMH Revision No:	3.0
Service :	N/A - Controlled document used across the organisation	Last Review Date :	1/04/2019
Document Owner:	Research Officer - Health Intelligence and Informatics	Next Review Date:	1/04/2022
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	21/05/2010
<i>If you are not reading this document directly from the Document Directory this may not be the most current version.</i>			

Associated Documents

Other documents relevant to this policy are listed below:

NZ Legislation	Privacy Act 1993 , The Health Information Privacy Code 1994 , The Official Information Act 1982 ,
CM Health Clinical Board Policies and Procedures	Clinical Audit Procedures Research Policy Research Approval and Study Closure Procedures , Disclosure of Health Information How a Third Party Requests Health Information About a Patient
Other related documents	Ministry of Health Working Party; Towards Clinical Excellence – An Introduction to Clinical Audit, Peer Review and Other Clinical Practice Improvement Activities 2002

Document ID:	A11138	CMH Revision No:	3.0
Service :	N/A - Controlled document used across the organisation	Last Review Date :	1/04/2019
Document Owner:	Research Officer - Health Intelligence and Informatics	Next Review Date:	1/04/2022
Approved by:	Clinical Governance Group (CGG)	Date First Issued:	21/05/2010
<i>If you are not reading this document directly from the Document Directory this may not be the most current version.</i>			

Policy: Auditing Access to Electronic Patient Records

Purpose

The purpose of this policy is to ensure a consistent approach to auditing and monitoring of electronic patient records systems and to outline the expected processes for follow up where unusual or unauthorised access is detected.

Scope

This policy is applicable to all staff who are involved in the auditing of electronic systems or in any subsequent follow up action. This group may include staff involved in auditing of clinical records (including the Quality Coordinator, Patient Information Services), service managers, HR managers, Privacy Officers, IT business managers and General Managers.

This policy does not apply to access that has been properly arranged in accordance with the Staff Portal policy.

Policy

Staff Requirements

CMDHB staff are only permitted to access clinical information systems and patient related information for the purposes of treating patients under their care or carrying out their duties as CMDHB employees. The [CMDHB Safe Management and Privacy of Personal Health Information Policy](#) states:

Personal health information is obtained and used for the purpose of providing ongoing care and treatment to the patients of CMDHB.

If a person wishes to obtain or use personal health information for a purpose other than that provided for in the policy, the policy states that that person ***must first seek the advice of their service manager or the Privacy Officer.***

[The Storage and Security of Electronic and Paper Clinical Records Procedure](#) states:

All incidents of failure to respect patient confidentiality are considered to be serious misconduct and will be formally performance managed.

This policy also states that it is considered misuse and unauthorised access if staff look up their own family members' / friends' results, appointments, referrals etc in the electronic or paper record without following the appropriate procedures for requests for information, including the processes set out in the Staff Portal policy.

The CMDHB Employment Privacy Agreement, signed by all staff, reinforces the above policies and further states that employees shall not:

Use or attempt to use any of the information specified above for the employee's own personal benefit, or for the benefit of any other person or organization, or in any manner whatsoever, other than in accordance with the employee's duties and consistent with the obligation of confidentiality expected for a person in the employee's position.

Document ID:	A5699	CMH Revision No:	1
Service :	Patient Information Services	Last Review Date :	2/04/2019
Document Owner:	Legal advisor	Next Review Date:	2/04/2022
Approved by:	Executive Leadership Team (ELT)	Date First Issued:	9/05/2007
<i>If you are not reading this document directly from the Document Directory this may not be the most current version.</i>			

Breaches of any of the above obligations will be considered to be serious misconduct. Employees under no circumstances should look at information of patients who are not in their direct clinical care.

CMDHB and the other Auckland Region DHBs have a “zero tolerance” approach to misuse of health information. Auditing of electronic systems is an essential aspect of the security required to maintain public confidence in our ability to keep health information safe.

CMDHB Requirements

CMDHB is required to work within the provisions of the Health Information Privacy Code 1994. Rule 5 of the Code requires health agencies to use such security safeguards as are reasonable in the circumstances to protect health information against unauthorised use, access or disclosure.

Auditing of electronic system access plays a key role in detecting misuse and deterring others from accessing information they are not entitled to view. The Interim Regional Information Sharing Guideline also establishes the following expectations in relation to information shared across DHBs:

It is recommended that 6 months of access transactions are audited for each user on an annual basis. The audit should focus on the user’s access to particular documents or records that do not fit the usual pattern of access for the individual user, taking into account the users surname, job role and location of work.

Further expectations are also set out in relation to audit of designated records such as those of celebrities, politicians and staff members within the organisation.

Audit Expectations

Systems

It is expected that monthly audit reports should be produced for electronic systems, where relevant, such as:

- Testsafe (community laboratory results)
- Éclair
- Concerto
- Any “break glass” access where this functionality exists
- Any other additional electronic systems implemented by CMDHB and recommended for inclusion on this audit schedule by the Auckland Region Privacy Advisory Group or the CMDHB Privacy Officer.

Document ID:	A5699	CMH Revision No:	1
Service :	Patient Information Services	Last Review Date :	2/04/2019
Document Owner:	Legal advisor	Next Review Date:	2/04/2022
Approved by:	Executive Leadership Team (ELT)	Date First Issued:	9/05/2007
<i>If you are not reading this document directly from the Document Directory this may not be the most current version.</i>			

Content of Reports

Where possible, reports should specifically identify the following events:

1. First name and surname of accessing staff member matches first name and surname of patient.
2. Surname of accessing staff member matches surname of patient.
3. Staff member has accessed records outside the service area within which he or she is employed.

Manual Checking

Manual checking of specific patient records and employee access logs should also occur. This includes checking of access to celebrity, high profile, politician and staff member clinical records as well as routine assessment of individual employee access logs.

Manual checking processes should include:

- consideration of usual patterns of access,
- identification of access occurring outside the normal parameters of use; and
- access that appears inconsistent with the user's role (e.g. an obstetric service staff member accessing the results of a male mental health client.)

Manual checking should occur in accordance with the schedule outlined in the associated Patient Electronic Record Audit Protocol.

Cross-Agency Auditing

Where audit logs are provided by other agencies (e.g. other Auckland region DHBs) then similar checks will be made to identify potentially inappropriate requests made by CMDHB staff members to access information held by those other agencies.

Follow up of Audit Results

Unusual Access to Third Party Information

If unusual or unexpected results are identified which indicate that there may have been access to another individual's information, and access cannot be understood by reference to the role of the staff member and the general information available about the patient then the "follow up process" should be followed (see appendix A).

An explanation should be sought directly from the staff member concerned. The Quality Coordinator, Patient Information Service, should notify the staff member's service manager and a letter seeking further explanation should be sent to the employee by the service manager, and copied to the Privacy Officer and relevant HR Manager for their information. It is important to remember that this is not a disciplinary process, although disciplinary action may follow if an adequate explanation is not provided by the employee.

Document ID:	A5699	CMH Revision No:	1
Service :	Patient Information Services	Last Review Date :	2/04/2019
Document Owner:	Legal advisor	Next Review Date:	2/04/2022
Approved by:	Executive Leadership Team (ELT)	Date First Issued:	9/05/2007
<i>If you are not reading this document directly from the Document Directory this may not be the most current version.</i>			

Explanation from Staff

Once a response is received from the staff member this should be carefully considered by the service manager. The service manager may need to seek further details or information regarding the nature of the access. If the response provides a valid and reasonable explanation for the access that occurred then no further action will be taken. If the staff member does not provide a reasonable explanation for the use that has occurred then the matter should be referred to the relevant HR manager for further action in accordance with the CMDHB discipline and dismissal policy.

Staff Accessing Own Information

Staff who wish to access their own information or results must make their requests through the usual DHB channels. They are not permitted to access their own information directly through CMDHB systems, unless access to such information has been arranged in accordance with the Staff Portal policy. Although outside the limits of acceptable use, access to a staff member's own results will ordinarily be regarded as an education matter, resulting in a reminder that such access is not acceptable and provision of information about the Staff Portal. Repeated access following a reminder being given may result in a more formal process being followed, in accordance with Appendix A.

Audit following Complaint or Concern

Process

If a complaint or concern relating to access to patient information arises the relevant service manager, general manager, clinical director or privacy officer can request an audit of the patient record or the employee access log from the Quality Co-Ordinator, Patient Information Service.

If any issues are identified from the audit these should be dealt with in accordance with the process outlined in this document for dealing with "unusual results" detected during routine audits.

Such investigation will be carried out as a part of, and in conjunction with, the usual complaints policy.

Reporting

Reporting of results

A monthly audit report will be compiled by the Quality Coordinator, Patient Information Service, outlining all instances of inappropriate access to clinical systems at CMDHB. This report will be provided to the Privacy Officer and relevant Human Resource Managers. Each incident in the report should be accompanied by a recommendation regarding the action that should be taken. Such recommendations will be in line with this policy.

Document ID:	A5699	CMH Revision No:	1
Service :	Patient Information Services	Last Review Date :	2/04/2019
Document Owner:	Legal advisor	Next Review Date:	2/04/2022
Approved by:	Executive Leadership Team (ELT)	Date First Issued:	9/05/2007
<i>If you are not reading this document directly from the Document Directory this may not be the most current version.</i>			

Summary reports will also be distributed by the Quality Coordinator, Patient Information Service. This summary report will outline:

- the number of exception reports identified for each service;
- the number of exception reports resulting in a “please explain” letter; and
- the number of exception reports resulting in referral to HR for disciplinary consideration.

This report will be circulated to the Health Information Committee and the MACS, for their month end reports. It will also be copied to the General Manager Clinical Support Services, Service Manager, Patient Information and the Privacy Officers.

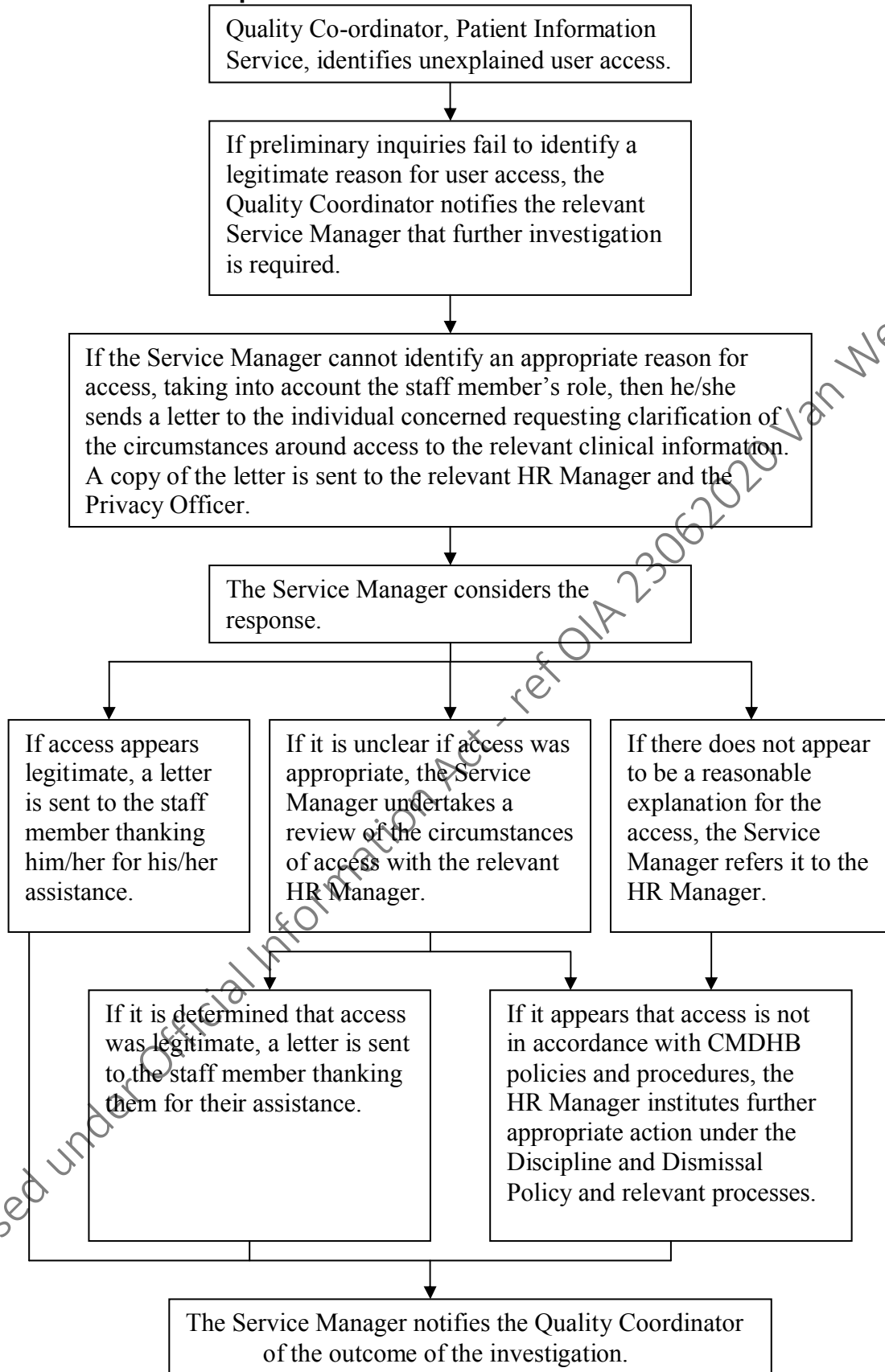
Associated Documents

Other documents relevant to this policy are listed below:

NZ Legislation	Privacy Act 1993 Health Information Privacy Code 1994
CMDHB Clinical Board Policies	Safe Management and Privacy of Personal Health Information Storage and Security of Clinical Records Code of Conduct Discipline and Dismissal Policy Staff Portal Policy – Use of Éclair for Accessing Own/Authorised Other’s test results
NZ Standards	New Zealand Standard 8153:2002 Health Records
Organisational Procedures	None
Other related documents	Code of Health and Disability Services Consumers’ Rights Employment Privacy Agreement signed by all staff

Document ID:	A5699	CMH Revision No:	1
Service :	Patient Information Services	Last Review Date :	2/04/2019
Document Owner:	Legal advisor	Next Review Date:	2/04/2022
Approved by:	Executive Leadership Team (ELT)	Date First Issued:	9/05/2007
<i>If you are not reading this document directly from the Document Directory this may not be the most current version.</i>			

Appendix A – Follow Up Process Flowchart
Unexplained Access to Clinical Information



released under Official Information Act - ref OIA 23062020 Van Wey Lovatt

Document ID:	A5699	CMH Revision No:	1
Service :	Patient Information Services	Last Review Date :	2/04/2019
Document Owner:	Legal advisor	Next Review Date:	2/04/2022
Approved by:	Executive Leadership Team (ELT)	Date First Issued:	9/05/2007
<i>If you are not reading this document directly from the Document Directory this may not be the most current version.</i>			

Policy: Fraud – Monitoring and Management

Background/Overview

Purpose

The purpose of this policy is to set out the CMDHB definition of fraud, its attitude towards fraud, and its procedures for investigating and dealing with fraud. It is intended to emphasise the responsibility of staff for reducing opportunities for fraud, and provide guidance on reporting of fraud and documentation of fraud investigation.



Note: This policy must be read in conjunction with the policies listed in the Associated DocumentsA section.

Scope of Use

This policy is applicable to all CMDHB employees (full time, part time and casual, temporary or seconded), Board members, contractors, visiting health professionals and students working in any CMDHB facility. For the purposes of this policy, the terms “employee and employees, and staff and staff members” include all the groups listed above.

Policy

Definition of fraud:

Fraud is an intentional or reckless act by one or more people involving the use of deception to obtain a benefit or that causes loss. Fraud includes any act intended to facilitate a fraud. The definition of fraud encompasses, but is not limited to the following behaviours:

- False accounting and/or the making of a false or misleading statement or claim, with a view to personal gain or gain for another person.
- Knowingly retaining a payment or benefit to which the employee knows he/she is not entitled.
- Assisting with or condoning fraud or dishonesty against CMDHB by another employee or external party.
- Theft or unauthorised personal use of CMDHB assets.
- Placing of a contract, or arranging the placing of a contract, with a particular supplier with a view to direct or indirect personal gain.
- Submitting a false timesheet, leave form or expense claim.

Document ID:	A5709	CMH Revision No:	4.0
Division :	Human Resources	Last Review Date :	11/10/2018
Document Owner:	Chief legal advisor	Next Review Date:	11/10/2021
Approved by:	Executive Leadership Team (ELT)	Date First Issued:	02/08/2007
Counties Manukau Health			

- Accepting and retaining a salary overpayment or leave balance to which the employee knows he/she is not entitled, and deliberately failing to report the overpayment or excess leave.
- Lying about credentials or qualifications.
- Using an official position to secure unwarranted benefits, privileges or profit.
- Disclosing confidential information to outside parties with a view to personal gain or gain for another person.
- Accepting or offering bribes or inducements.
- Forgery or unauthorised alteration of any document belonging to the DHB with a view to personal gain or gain for another person or which causes loss to any person including CMDHB.
- Issuing false or misleading invoices.
- Stealing records, equipment or any item belonging to the DHB.
- Unauthorised personal use of the CMDHB vehicles or other assets.
- Granting a contract, or facilitating or procuring the granting of a contract, to a particular person or company with a view to direct or indirect personal gain, or which causes loss to any person including CMDHB.

CMDHB's attitude towards fraud

CMDHB regards fraud and fraudulent behaviour as totally unacceptable. Any employee who suspects any fraudulent activity involving CMDHB in any way must report it to their GM in the first instance, unless they suspect their GM's involvement, in which case it must be reported to the CFO.

All allegations of fraud will be taken seriously and properly and fully investigated. Any matter that suggests fraud on the part of any employee will be properly and fully investigated and, if substantiated, may result in disciplinary action against the applicable employee(s). Any substantiated allegations of fraud may be reported to the police and/or the Serious Fraud Office and/or the Office of the Auditor-General for further investigation and possible prosecution.

Wherever possible and practical, recovery of the lost money or other property will be pursued.

If a staff member is asked to provide a reference for an employee who was dismissed in connection with fraud, he/she must seek advice from the DHB legal adviser before any reference (whether written or verbal) is provided.

Document ID:	A5709	CMH Revision No:	4.0
Division :	Human Resources	Last Review Date :	11/10/2018
Document Owner:	Chief legal advisor	Next Review Date:	11/10/2021
Approved by:	Executive Leadership Team (ELT)	Date First Issued:	02/08/2007
Counties Manukau Health			

The CMDHB attitude to fraud described above, and the processes outlined in this policy regarding reporting of fraud, is an approach that CMDHB will apply consistently. The principles will apply to all allegations of fraud. This includes situations where the fraud or alleged fraud has been committed against CMDHB by an organisation, or an individual associated with such an organisation, that is contracted to or funded by CMDHB.

Staff responsibilities

CMDHB employees must exhibit the highest standards of honesty and integrity in their dealings with patients, suppliers, contractors, other health service providers and their fellow employees. They must seek the best possible value for the taxpayers' dollars. They must not seek or accept unauthorised personal benefits.

Staff must take reasonable steps to safeguard CMDHB funds and assets against fraudulent, unauthorised use and misappropriation. Staff members must report suspected fraud and/or breakdowns in internal control systems to their managers.

Management responsibilities

Each RC Manager / Service Manager / General Manager is responsible for ensuring controls are implemented and monitored that safeguard against fraudulent activity in their areas of responsibility.

Managers need to ensure employees are informed of, and conform to, applicable policies and procedures and receive appropriate training in internal control.

It is also management's responsibility to identify weakness in internal control systems and follow these up with corrective action.

Managers may call on the support of the Regional Internal Audit Service if they require assistance to evaluate or improve internal control systems.

Internal controls

CMDHB is committed to the development and maintenance of effective internal control systems to prevent and detect fraud. Examples of internal controls include, but are not limited to:

- Segregation of duties: at least 2 people, acting independently, must be involved in the approval or purchasing, finance, payroll, work related expenses, and human resources transactions.
- Performance of thorough background checks when recruiting employees including checking criminal records, checking references and verifying qualifications.

Document ID:	A5709	CMH Revision No:	4.0
Division :	Human Resources	Last Review Date :	11/10/2018
Document Owner:	Chief legal advisor	Next Review Date:	11/10/2021
Approved by:	Executive Leadership Team (ELT)	Date First Issued:	02/08/2007
Counties Manukau Health			

- Documentation of financial transactions so that they can be traced through an adequate paper trail.
- Implementation of systems and procedures for verifying timesheets and leave forms, and the overpayment requirements detailed in the Overpayment policy.
- Credit card use limitations and checks, as detailed in the Credit Card Usage policy and procedure.
- Requirements that no staff member may approve their own time sheet, leave application or expense claim, nor may they purchase an asset for their own use, without their manager's approval.

Detection and Investigation – Recommended Process

The table below sets out the recommended process to properly and fully investigate any allegation of fraud. The actions must be taken as soon as possible. The use of the process below is recommended to ensure that any alleged fraud is properly and fully investigated and every individual suggested to be involved in any fraud is dealt with in a fair, proportionate and consistent manner.

Staff are also entitled to report suspected fraud in accordance with the Protected Disclosures Policy.

Fraud may also be reported directly to The Ministry of Health (Health Integrity Line) at any time. In any investigation process, the relevant Human Resources Manager and the DHB Legal Adviser must be involved in planning and implementation of the investigation process. This will ensure that appropriate employment obligations and all legal requirements are considered.

When fraud is alleged, all concerns must be thoroughly documented by the person to whom the report is made. Thorough and complete records of the following steps taken must also be made. Documentation is the responsibility of everyone involved in the detection and investigation process.

If the staff member suspects fraud by:	They should report it to:	The means by which the allegation will be investigated and documented (including involvement of the Police and/or Serious Fraud Office and/or the Auditor-General) will be decided by:
A contractor, a supplier or an employee of a supplier	Their General Manager. (The GM <u>must</u> report the allegation promptly to the CFO)	The CFO after consultation with the Regional Internal Audit Manager.

Document ID:	A5709	CMH Revision No:	4.0
Division :	Human Resources	Last Review Date :	11/10/2018
Document Owner:	Chief legal advisor	Next Review Date:	11/10/2021
Approved by:	Executive Leadership Team (ELT)	Date First Issued:	02/08/2007
Counties Manukau Health			

Policy: Fraud – Monitoring and Management

Another staff member (other than their General Manager or the Chief Executive or the Chief Financial Officer or the Chief Operating Officer)	Their General Manager. (The GM <u>must</u> report the allegation promptly to the CFO)	The CFO after consultation with the Regional Internal Audit Manager. HR advice should also be sought.
A General Manager	The Chief Executive. (The Chief Executive <u>must</u> report the allegation promptly to the CFO, the Regional Internal Audit Manager and the Chair of the Board)	The CEO after consultation with the CFO and the Regional Internal Audit Manager. HR advice should also be sought.
The Chief Executive and/or the Chief Financial Officer and/or the Chief Operating Officer	The Chair of the Board. (The Chair <u>must</u> report the allegation promptly to the Regional Internal Audit Manager and the External Auditor. If there are prima facie indications that the allegation may have substance the Chair must also report it to the Minister of Health)	The Chair after consultation with the Regional Internal Audit Manager and the External Auditor. HR advice should also be sought.
The Chair of the Board and/or another board member	The Chief Executive (The Chief Executive <u>must</u> report the allegation promptly to the Manager of the Regional Internal Audit Service and the External Auditor. If there are prima facie indications that the allegation may have substance the Chief Executive must also report it to the Minister of Health)	The Minister of Health and/or the Office of the Auditor-General

The person to whom the allegation of fraud is made should consider whether it is appropriate to refer investigation of the alleged fraud to an external agency.

Notification of alleged fraud

CMDHB will not hesitate to report alleged fraud to the police and/or the Serious Fraud Office and/or the Office of the Auditor-General for further investigation and possible prosecution. In addition, the notification must be made to:

- The Audit and Finance Committee (of the outcome).
- The external auditor (of the outcome).
- The insurer (of any investigation, if CMDHB may need to make an insurance claim).

References

Definitions/Description

Associated Documents

Document ID:	A5709	CMH Revision No:	4.0
Division :	Human Resources	Last Review Date :	11/10/2018
Document Owner:	Chief legal advisor	Next Review Date:	11/10/2021
Approved by:	Executive Leadership Team (ELT)	Date First Issued:	02/08/2007
Counties Manukau Health			

Other documents relevant to this policy are listed below:

NZ Legislation	Crimes Act 1961 Secret Commissions Act 1910 Protected Disclosures Act 2000
CMDHB Clinical Board Policies	<ul style="list-style-type: none"> ▪ Complaints Process and Resolution - Policy ▪ Complaints Process and Resolution - Procedure
Organisational Procedures	<p>Corporate Policies and Procedures</p> <ul style="list-style-type: none"> ▪ Credit Card Usage ▪ Employee Travel and Conference Attendance ▪ Entertainment ▪ Petty Cash ▪ Work Related Expenses ▪ Media <p>Human Resources Policies and Procedures</p> <ul style="list-style-type: none"> ▪ Conflict of Interest ▪ Discipline and Dismissal ▪ Exit and Termination ▪ Overpayment ▪ Protected Disclosures ▪ Recruitment
Other related documents	<p>AG-206: Auditor General's statement on the auditor's responsibility to consider fraud in an audit of a financial report.</p> <p>Report of the Controller and Auditor General: Central Government – Results of the 2003-2004 Audits.</p>

Definitions

Terms and abbreviations used in this document are described below:

Term/Abbreviation	Description
Fraud	An intentional act by one or more people involving the use of deception to obtain an unjust or illegal advantage.

Document ID:	A5709	CMH Revision No:	4.0
Division :	Human Resources	Last Review Date :	11/10/2018
Document Owner:	Chief legal advisor	Next Review Date:	11/10/2021
Approved by:	Executive Leadership Team (ELT)	Date First Issued:	02/08/2007
Counties Manukau Health			