POLICY

CONFIDENTIALITY & PRIVACY POLICY	
Applicable to: **All Employees**	Issued by: **Human Resources and Organisational Development**
	Contact: **Human Resource Consultants**

1. PURPOSE

The purpose of this policy is to:

- Ensure the confidentiality of MidCentral District Health Board's clinical and non-clinical information is maintained, including data collected that is specific to individual health professionals.
- Give guidance to all employees of MidCentral District Health Board (MDHB), including honorary staff members, students, volunteers and contractors about their obligations to maintain the confidentiality of all information that is held or owned by MDHB, including information about patients and clients.
- Set out the process that must be followed if a confidentiality or privacy breach occurs.

2. SCOPE

This Policy applies to all **employees** of MDHB (see definition below) – both during and subsequent to their employment/engagement with MDHB.

The requirements in this Policy apply to all **Confidential Information** (see definition below).

3. ROLES & RESPONSIBILITIES

All employees must maintain the security of confidential information which is held or owned by MDHB in accordance with their obligations and the requirements set out in this Policy.

All employees are expected to understand and comply with the requirements of the Privacy Act 1993 and the Health Information Privacy Code 1994 and with any relevant professional obligations relating to the confidentiality or protection of information (including Codes of Practice or Conduct that are issued by health practitioner registration authorities or other professional bodies).

To avoid doubt, the requirements in this Policy are in addition to the minimum requirements set out in the Privacy Act and the Health Information Privacy Code, professional obligations, and any other obligations imposed by law.

Any breach of this Policy or of the terms of the MDHB Declaration of Confidentiality, if substantiated after investigation, may provide grounds for disciplinary action, which may result in a disciplinary outcome up to and including summary dismissal.

Any breach of this Policy by people who have left the employ of MDHB, or who are no longer contracted or "engaged" by MDHB, may provide grounds for legal action.

© MidCentral District Health Board 2017. **CONTROLLED DOCUMENT.** The electronic version is the most up-to-date version. MDHB will NOT take any responsibility in case of any outdated paper copy being used and leading to any undesirable consequence.
Printed 19/11/2019 3:17:00 p.m.

MDHB collects and uses clinical information and data that relates to its employees, including health professionals, for the purposes of planning and delivery of services. This information has other applications within the DHB, including operational and contractual uses, for example, job sizing.

MDHB will maintain confidentiality of clinical information and data collected for this purpose and the release of any such information external to MDHB will generally be aggregated and/or anonymised, unless otherwise required by legislation or another external party, for example the Ministry of Health, Health and Disability Commissioner, or Ombudsman.

4. POLICY

"**Employees**" (see definition below) may receive, observe or otherwise have access to "**Confidential Information**" (see definition below) by virtue of their presence on MDHB premises or their employment or contractual relationship with MDHB.

To protect Confidential Information, all employees must understand and adhere to the following requirements:

(a) Employees may only access, use or disclose Confidential Information as is necessary to meet their employment or contractual obligations with MDHB and in accordance with the Privacy Act, the Health Information Privacy Code, their professional obligations, and any other obligations imposed by law. Specifically, Confidential Information concerning a patient or client who is receiving or has received services provided by MDHB may not be accessed by employees not involved in the care or treatment of the patient or client, and also may not be disclosed to unauthorised persons. Note: This does not preclude the sharing of clinical information among health professionals involved in the care or treatment of the individual on a "need to know" or consultancy basis, or where accessing patient information is part of an employees role, for example for audit purposes, and for quality/risk/information technology.

(b) Other than in accordance with paragraph (a) above or where one of the exceptions set out below in (c) applies, employees must treat all Confidential Information as strictly confidential and may not access, use or disclose it in any way.

(c) Employees **may** disclose Confidential Information where:

(i) The source of the information is a publicly available publication and, in the circumstances, it would not be unfair or unreasonable to disclose the information; or
(ii) They have express permission in writing from their manager; or
(iii) They believe the information needs to be disclosed in order to participate in a Protected Quality Assurance Activity (as defined in the Health Practitioners Competence Assurance Act 2003); or
(iv) They believe disclosure of Confidential Information is required as part of a disclosure under the Protected Disclosures Act 2000; or
(v) They are otherwise legally required to disclose the information.

(d) Employees must take care to ensure that all materials, including all documents provided to them in the course of their employment or contractual obligations which contain Confidential Information are kept securely and are not accessed by, disclosed to or duplicated for any person, corporate entity, firm or organisation **unless** they have prior written authorisation from their manager.

All employees are required to sign and adhere to the terms set out in the "MDHB Declaration of Confidentiality" document (Appendix 1 of this Policy).

The MDHB Declaration of Confidentiality will be included with the employment agreement for all new employees and, as a condition of their employment, the Declaration must be signed before the employee takes up his or her appointment.

At the request of MDHB, at any time, employees will promptly deliver to MDHB all Confidential Information disclosed to them without retaining any copies, or, (at MDHB's election) destroy that Confidential Information in a manner as MDHB may direct. MDHB may require reasonable evidence from the employee that they have complied with this provision including a certificate to that effect signed by the employee.

Where Confidential Information must be disclosed as required by law, employees:

- Must notify their manager about the Confidential Information that is to be disclosed (and of the circumstances in which the disclosure is required) before disclosing the information; and
- Will only disclose the extent of information that is necessary in the circumstances.

Employees must understand that:

- Any waiver of the terms in this Policy must be in writing and signed by the Chief Executive Officer (or nominee) at MDHB;
- The obligations set out in this Policy and in the MDHB Declaration of Confidentiality will survive the terms of the employee's engagement or any other contractual obligations; and
- The obligations of confidentiality imposed by this policy are in addition to obligations of confidentiality otherwise imposed by law, or imposed by the employee's professional bodies or associations.

Neither this policy nor the MDHB Declaration of Confidentiality is intended to unreasonably restrict employees from exchanging ideas relating to their expertise, experience and employment with professional colleagues elsewhere. However, as in all circumstances, compliance with the Health Information Privacy Code and Privacy Act is required.

Confidentiality or Privacy Breaches

Employees are expected to report any actual or suspected breaches of this Policy. This includes breaches of privacy ("**Privacy Breach**" – as defined below) and the theft, loss or unauthorised disclosure of or access to "**Confidential Information**".

All reports must be made using MDHB's incident reporting system or an alternative reporting mechanism as may be appropriate depending on the circumstances. Employees may report actual or suspected breaches without any fear of reprisal.

All reports will be promptly assessed and addressed for containment, investigation, reporting, and remedial actions.

In respect of a "**Privacy Breach**", guidance material issued by the Privacy Commissioner recognises that managing a privacy breach has four stages:

- Containing the breach and preliminary assessment;
- Evaluating the risks;
- Considering or undertaking notification; and
- Putting in place future prevention strategies.

The checklist in Appendix 2 is to be used as a guide for managing an actual or suspected "**Privacy Breach**". This checklist can also be used as guidance in the event of the theft, loss or unauthorised disclosure of or access to other "**Confidential Information**".

5. DEFINITIONS

Employees: All past, present and future employees of MDHB, including honorary staff members, students, volunteers and contractors working for MDHB or at MDHB sites.

Confidential Information: Includes, but is not limited to:

- "**Health Information**" as defined below;
- "**HR Information**" as defined below; and
- "**Business Information**" as defined below.

Health Information: means any information about past, present or future MDHB patients or clients, and, for the avoidance of doubt, includes health information about patients or clients who are also MDHB employees.

HR Information: means personal information about past, present or future employees that relates to their employment or contractual relationship with MDHB.

Business Information: means all information relating to MDHB business matters, including but not limited to:

- trade secrets, contracts, confidential operations, processes or dealings, including any confidential incident reviews or other reports;
- any information concerning the organisation, business, finances, transactions or affairs of MDHB, its services or its institutions; and
- any data that has been deemed commercial in confidence by the Chief Executive Officer.

To avoid doubt, **"Information"** means any information and may take the form of, among other things, conversations, records, notes, emails, personal details and statistics held by MDHB in hard-copy format or electronic form (accessed through a computer or other similar electronic device or system).

Confidentiality Breach: is the result of unauthorised access to, or collection, use or disclosure of "**Confidential Information**" (as defined above).

Privacy Breach: is the result of unauthorised access to, or collection, use or disclosure of, personal information, including but not limited to Health Information and HR Information. In this context, "unauthorised" means in contravention of the Privacy Act 1993. Privacy breaches can occur in a number of ways, some examples are:

- Individuals can deceive agencies into improperly releasing the personal information of another;

- Laptops, removable storage devices, or physical files containing personal information are lost or stolen;
- An agency mistakenly provides personal information to the wrong person, for example by sending details out to the wrong address;
- Employees accessing personal information outside of the requirements of their employment.

6. RELEVANT LEGISLATION

Privacy Act 1993
Health Information Privacy Code 1994
The Official Information Act 1982
Public Records Act 2005
Health Act 1956

Copies of relevant Acts are available online at www.legislation.govt.nz.

7. RELATED MDHB DOCUMENTS

MDHB-5582	Code of Conduct [Policy]
MDHB-1889	Disciplinary Procedures [Policy]
MDHB-1943	Information Systems Security and Access [Policy]
MDHB-5365	Email [Policy]
MDHB-5366	Internet - Acceptable Use [Policy]
MDHB-2053	Disclosure of a Serious Wrongdoing (Whistle Blowing) [Policy]
MDHB-4873	Protected Quality Assurance Activities (PQAA) [Policy]
MDHB-673	Health Information Access Release Disclosure [Policy]
MDHB-5797	Health Information Access Release Disclosure [Procedure]
	Collective/Individual Employment Agreements

8. APPENDICES

Appendix 1:	MDHB Declaration of Confidentiality
Appendix 2:	Checklist for Privacy/Confidentiality Breaches

9. KEYWORDS

Confidentiality
Privacy
Privacy breach
Security of information
Accessing information
Disclosing information

APPENDIX 1

MDHB DECLARATION OF CONFIDENTIALITY

I, _____(print name), confirm the following:

1. I understand that MidCentral District Health Board "MDHB" has a Confidentiality & Privacy Policy ("the Policy") that covers "Confidential Information".

2. I understand that "**Confidential Information"** includes, but is not limited to:
   - "**Health Information**" as defined below;
   - "**HR Information**" as defined below; and
   - "**Business Information**" as defined below.

   Health information: means any information about past, present or future MDHB patients or clients, and, for the avoidance of doubt, includes health information about patients or clients who are also MDHB employees.

   HR Information: means personal information about past, present or future employees that relates to their employment or contractual relationship with MDHB.

   Business Information: means all information relating to MDHB business matters, including but not limited to:
   - trade secrets, contracts, confidential operations, processes or dealings, including any confidential incident reviews or other reports;
   - any information concerning the organisation, business, finances, transactions or affairs of MDHB, its services or its institutions; and
   - any data that has been deemed commercial in confidence by the Chief Executive Officer.

3. I understand that I must comply with the requirements set out in the Policy, but in particular I understand that:

   (a) I may only access, use or disclose Confidential Information as is necessary to meet my employment or contractual obligations with MDHB and in accordance with the Privacy Act 1993, the Health Information Privacy Code 1994, my professional obligations, and any other obligations imposed by law.

   (b) I may only access, use or disclose to authorised persons Confidential Information concerning a patient or client who is receiving services provided by MDHB when I am involved in the care or treatment of the patient or client, or if my role within MDHB requires that I do so.

   (c) Other than in accordance with paragraph (a) above or where one of the exceptions set out below in (d) applies, I must treat all Confidential Information as strictly confidential and I may not access, use or disclose it in any way.

   (d) I **may** disclose Confidential Information where:

      (i) The source of the information is a publicly available publication and, in the circumstances, it would not be unfair or unreasonable to disclose the information; or

(ii) I have express permission in writing from my manager; or
(iii) I believe the information needs to be disclosed in order to participate in a Protected Quality Assurance Activity (as defined in the Health Practitioners Competence Assurance Act 2003); or
(iv) I believe disclosure of Confidential Information is required as part of a disclosure under the Protected Disclosures Act 2000; or
(v) I am otherwise legally required to disclose the information (in which case, I understand that I must notify my manager about the Confidential Information that is to be disclosed, and the circumstances in which disclosure is required, before disclosing the information, and I will only disclose the extent of information that is necessary in the circumstances).

(e) I must take care to ensure that all materials, including all documents provided to me in the course of my employment or contractual obligations which contain Confidential Information are kept securely and are not accessed, disclosed to or duplicated for any person, corporate entity, firm or organisation **unless** I have prior written authorisation from my manager.

4. I understand that the requirements in the Policy are minimum requirements, and that I must also comply with all relevant legal requirements, including the requirements that are set out in the Privacy Act 1993 and the Health Information Privacy Code 1994 and any relevant professional obligations that I have relating to the confidentiality or protection of information.

5. I understand that any breach of the Policy, if substantiated after investigation, may provide grounds for disciplinary action, which may result in a disciplinary outcome up to and including summary dismissal, or legal action as appropriate.

6. I know that if I am unsure about the requirements in the Policy I should seek advice from my manager or other appropriate senior MDHB employees.

7. I understand that the requirements in the Policy survive the terms of my engagement with MDHB.

_____ _____
(Signed) (Date)

WITNESSED BY:

_____ _____
(Signature) (Date)

_____ _____
(Full Name) (Occupation)

APPENDIX 2

CHECKLIST FOR PRIVACY/CONFIDENTIALITY BREACHES

	Notes
Containing the breach and preliminary assessment	
☐ Have you contained the breach (recovery of information, computer system shut down, locks changed, permissions changed)? ☐ Have you designated an appropriate person to lead the initial investigation? ☐ Is there a need to have a meeting and discuss with a wider group of staff? Who should be included, for example, privacy officer, security, communications, Human Resources, Operations Director, risk management, legal team? ☐ Have you determined who needs to be made aware of the incident internally and potentially externally at this stage? ☐ Does the breach appear to involve theft or criminal activity? If yes, have the police been notified? ☐ Have you made sure the evidence that may be necessary to investigate the breach is preserved? ☐ Have you completed an incident report within the organisation's incident reporting system (or alternative reporting mechanism, as may be appropriate depending on the circumstances)?	
Evaluate the risk	
☐ What personal information was involved? o For example, name, address, unique identifiers, financial or medical information? o What form was the information in, for example, paper record, electronic? o What physical or technical security measures were in place at the time of the incident, for example, locks, alarm systems, encryption, passwords? ☐ What was the cause and extent of the breach? o Is there a risk of ongoing breaches or further exposure of the information? o Can the personal information be used for fraudulent or other purposes? o Was the information lost or stolen? If it was stolen, can it be determined whether the information was the target of the theft or not? o Has the personal information been recovered? o Is this a systemic problem or an isolated incident? ☐ How many individuals have been affected by the breach and who are they? o Establish who, and how many individuals have been affected by the breach. o Consider open disclosure and whether this is appropriate for this incident. ☐ Is there any foreseeable harm for the breach? o What harm to the individuals could result from the breach? For example, security risk, financial loss, identity theft, physical harm, significant humiliation or loss of dignity, or	

damage to reputation and relationships. ○ Do you know who has received the information and what is the risk of further access, use or disclosure? ○ What harm to the DHB could result from the breach, for example, loss of trust, financial exposure, health issue exposure, legal proceedings, complaint? ○ What harm could come to the public as a result of notification of the breach, for example, risk to public health or safety.	
Notification	
☐ Should affected individuals be notified? ○ What are the reasonable expectations of the individuals concerned? ○ What is the risk of harm to the individual? Is there a risk of physical harm? ○ What are the legal and contractual obligations of the DHB, for example, open disclosure policy? ○ If you decide that affected individuals do not need to be notified, record your reasons on the incident form within the organisation's incident reporting system. ○ If affected individuals are to be notified, when, how and who will notify them? ○ What form of notification will you use, for example, phone, letter, email or in person? ○ Who will notify the affected individuals? Do you need to involve another party? ○ What should be included in the notification, for example: information about the incident and its timing in general terms; a description of the personal information involved in the breach; a general account of what the DHB has done to control or reduce the harm; what the DHB will do to assist individuals in the reduction of harm; sources of information that may assist individuals; and contact information of the department or staff member within the DHB who can answer questions or provide further information. ○ Should the Privacy Commission be made aware of the breach? ○ Inform the individuals concerned of their right to make a complaint.	
Prevention of future breaches	
☐ What steps can you take short or long term to change practice? ○ What is required to correct the situation, for example, staff training, policy or procedure development or review? ○ Who needs to be involved in this process, for example, the service involved, discipline involved, Quality and Clinical Risk Coordinators? ○ What tools will you use to map out the changes to practice? For example Plan, Do, Study, Act (PDSA) cycle, action plan? ○ Do you need to audit the process change in 3, 6 or 12 months to ensure the changes are fully embedded within the service or discipline?	