Canterbury District Health Board
Te Poari Hauora ō Waitaha

West Coast District Health Board
Te Poari Hauora a Rohe o Tai Poutini

CORPORATE OFFICE

Level 1
32 Oxford Terrace
Christchurch Central
CHRISTCHURCH 8011

Telephone: 0064 3 364 4160
Fax: 0064 3 364 4165
carolyn.gullery@cdhb.health.nz

14 July 2020

Ms Amy S Van Wey Lovatt

Email: fyi-request-12922-4e5afdf5@requests.fyi.org.nz;

Dear Ms Van Wey Lovatt

RE Official information request CDHB 10340 & WCDHB 9440

I refer to your email dated 17 June 2020 to the Ministry of Health, which they have subsequently partially transferred to us on 24 June 2020, requesting the following information under the Official Information Act from Canterbury DHB and West Coast DHB. Specifically:

DHB policies in regard to reporting unsafe, harmful, criminal behaviour, including the re-routing and interception of private communications, and policies on how they document such incidents and how they are to safeguard against such incidents.

Please note: The policies outlined below are currently being reviewed and updated, and when completed they will all cover both Canterbury DHB and West Coast DHB.

Please find attached:

1. **Appendix 1** – Incident Management Policy (Canterbury DHB and West Coast DHB)
2. **Appendix 2** – Information Security Management Policies (Canterbury DHB only)
3. **Appendix 3** – Information Management Policy (Canterbury DHB and West Coast DHB)
4. **Appendix 4** – Disclosure of Adverse Patient Events Procedure (West Coast DHB only)
5. **Appendix 5 –** Access Control (ICT) Policy (Canterbury DHB and West Coast DHB)
   - Overarching policy statement – "All users must be authorised and must only view and process the information they are entitled to and have a need to access"
   - Responsibilities – "Any person with access to DHB information systems MUST comply with all USER policies in this document and any confidentiality and disclosure agreements they may be asked to sign"
   - Non-compliance – "In the event that an account or password is suspected to have been compromised, the incident must be reported to ISG Service Desk immediately"
   - Authorised Use:
     i. "DHB information systems may only be used for the purpose intended and by authorised personnel.
     ii. DHB information systems must not be used for non-DHB purposes including soliciting business, selling products or services, or otherwise engaging in commercial activities, other than those expressly permitted by Executive Management Team Members or General Managers.
     iii. Users of a DHB information system may not gain unauthorised access to any other DHB or regional information system, or in any way disclose, damage, alter or disrupt the information on it, or the operation of the system.
     iv. Users are prohibited from exploiting vulnerabilities or deficiencies in information security, capturing or otherwise obtaining passwords, or the use of any other access mechanism, which could permit unauthorised access.
     v. Failure to comply with these conditions will result in disciplinary action being taken."
6. **Appendix 6** – Incident Handling Policy (Canterbury DHB only)

I trust that this satisfies your interest in this matter.

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

Yours sincerely

Carolyn Gullery
Executive Director
Planning, Funding & Decision Support

Contents

Purpose

Canterbury District Health and West Coast District Health Boards aim for zero harm occurring to any person within our facilities or care. Implementation of this policy contributes to meeting current legislative requirements, standards (e.g. HDSS 2.4, NZS8134:1:2008) and the Health and Quality Safety Commission (HQSC) Health and Disability Services' National Reportable Events Policy 2012.

Policy

Both the Canterbury District Health Board (DHB) and the West Coast Health Board (WCDHB) are committed to providing safe environment for all individuals. Leadership, education and training, role clarity, teamwork, well designed processes, relevant metrics, and regular feedback are essential for safety in any system. Promotion of safety and prevention of harm must be the first consideration in all actions. However, we recognise that incidents happen and need to be managed effectively to prevent recurrence in the future.

When an incident occurs, immediate remedial action with open disclosure and regular communications with patient/ family/ whanau/ staff through to closure of the incident must be the norm.

These DHBs' promote just cultures, with the focus of any response being on the 'what and how' an incident happened and not on 'who' made an error.

The ability to continuously assure and systematically learn and improve system safety is reliant on having all incidents and 'near misses' accurately recorded. An appropriate level of investigation is then conducted in a timely manner to learn and improve the system, and provide timely information to those involved, services and relevant agencies.

Scope

Inclusion

Applies to all Canterbury and West Coast DHB staff, inclusive of honorary or unpaid employees, temporary employees, students, volunteers, contractors and any other persons working for, or providing services to, these two DHBs'.

This scope includes incidents identified in the respective services and sites and/or during the performance of duties in both clinical and non-clinical settings, and those discovered through reports, team discussions, observation, complaints, audits and other forms of chart review, and reporting for other purposes.

For brevity, the use of the term 'incident' represents both 'incident' and 'near miss' in this policy and the pluralism of DHBs' refers specifically to Canterbury and the West Coast District Health Boards.

Exclusion

Employee incidents are managed under the Health Safety and Wellbeing Policy.

Employment relationship issues are managed under the Employment Relations Act 2000 (and regulations).

Roles and Responsibilities

Our Workforce

- Work to minimise the occurrence of incidents and continuously improve services.
- Take immediate action to reduce any consequences of an incident, and support open disclosure with patient and/or family.
- Notify all incidents to the clinical leader/ manager at the time and enter incidents into the electronic incident recording system and record fully in clinical notes.
- Participate in the review of an incident and implementation of recommendations made, as requested by their manager, completing any requested activity in a timely manner.

  Note: People involved in an incident review are entitled to have a support person of their choice accompany them during interviews.
- Encourage colleagues to report incidents that have been identified.
- Complete an incident form for incidents involving volunteers or other personnel working or providing services to Canterbury DHB.

Clinical Leaders/Managers

For purposes of this policy, is any employee with supervisory responsibilities or line management of any area. In addition to the workforce responsibilities above, clinical leaders/managers:

- Promote excellence, safety, teamwork, open disclosure, learning, and continuous improvement.
- Address the affected person and their family's needs as a priority during the incident management process. This includes timely, co-ordinated communication and development of a meaningful investigation report.
- Ensure appropriate support of staff, and notified appropriate agency personnel when an incident involves a student, (see Appendix 1).
- Manage and review incidents to the required standard within timeframes. Complete hazard registers as necessary.
- Ensure staff have adequate training and are aware of their responsibilities with regard to notifying, and management of incidents and open disclosure.
- Check the accuracy of data, manage access and keep data secure so that privacy and confidentiality requirements for patients and employees are met.
- Ensure that an agreed single point of contact has been identified (either the responsible clinician or a member of the incident review team) who will:
  - keep the patient or the spokesperson for the family briefed on progress throughout the incident review process at regular agreed intervals (at least monthly)
  - arrange for the review team to discuss the final outcome and review report with the patient/family
- Ensure where serious harm has occurred, they contact the appropriate person in charge/ Clinical Lead/ Manager and Department Lead (i.e. Quality and Patient Safety) as soon as practicable who will report incidents to appropriate departments and senior leaders.

- Notify and seek advice from Quality and Patient Safety Teams, Legal team and senior line managers when handling complex matters.
- Ensure clinical governance activities are robust at department and service level. They include monitoring, trending, and constructively using incident, complaints and risk data in system improvement and workforce development.

Quality and Patient Safety Teams

- Provide advice and support to clinical leaders and managers and consult with the Legal Team and senior line managers as required, when handling complex matters.
- Support clinical leaders and managers to ensure the quality of management and review of incidents is to an appropriate standard and completed within set timeframes.
- Provide incident management education and training.
- Ensures processes are in placed so all SAC 3 and 4 Incidents are investigated within 30 calendar days at a divisional level and are closed off by the file manager's manager or designated quality staff.
- Ensure there is a process in place for accuracy of data, manage access and keep data secure so that privacy and confidentiality requirements for patients and employees are met (see Appendix 2).
- Support clinical leaders, managers, clinical governance committees to promote improvement, analyse, monitor, and improve outcomes and safety, and reduce risk. This includes ensuring the use of incident data is for improvement purposes, and not used to the detriment of individuals or services.
- Ensure processes are in place and used to monitor, analyse, and compile divisional reports on incident rates, types, trends and implementation of recommendations and escalate concerns to Clinical Governance bodies.

Serious Harm

- Co-ordinate serious incident reviews using standard processes and templates, monitoring timeliness of report completion, implementation of recommendations and review sign off by the relevant General Manager.
- Ensure that an agreed single point of contact has been identified (either the responsible clinician or a member of the incident review team) who will:
  - keep the patient or the spokesperson for the family briefed on progress throughout the incident review process at regular agreed intervals (at least monthly)
  - arrange for the review team to discuss the final outcome and review report with the patient/family as appropriate
- The members of the CDHB and the WCDHB Serious Incident Review Committees must be notified of a Serious Adverse Event (SAC 1 and 2). A Reportable Event Brief (REB) must be completed and attached to the file within 5 working days.

  All serious adverse events require a Serious Event Review to be completed within 70 calendar days of notification of the incident. The review approach is decided by the senior team. The report is approved for release by the appropriate General Manager when completed and the event is signed off when the recommendations have been implemented.

- Ensure evaluation of implemented recommendations from serious harm events occurs within 3 months of completion.

Clinical Governance Committees
In addition to the above:

- Ensure services have adequate clinical governance and risk management processes in place.
- Are proactively promoting safety, reducing risk and sharing learnings.
- Oversee the monitoring of the implementation of recommendations that arise from:
  - Serious Event Review Reports, Coroner reports, Health & Disability Commissioner.
  - ACC treatment injury reports.
  - Trigger Tools.
  - Hazard identification.
- Monitor timeliness of reporting, data accuracy and completion, closure and implementation of recommendations.
- Monitor incident types, trends, recommendation themes and consider how best to approach improvement.
- Embed learnings through systemic change in organisational processes and workforce development systems. Incorporate potential systemic improvement into organisational planning processes.

General Managers

- Ensure clinical governance groups are fully functioning and achieving their terms of reference.
- Monitor serious incident investigation quality, timeliness of reporting, and implementation of recommendations.
- Work with clinical leads and Quality Teams to approve and sign off serious event review reports.
- Sign off serious event reviews following implementation of recommendations, approve closure to Serious Event Review Committees.
- Support monitoring of improvements to ensure sustainability.

Quality and Patient Safety - Corporate

- Has responsibility for application systems administration, upgrades, and assuring governance processes (see Appendix 2).
- Works with regional partners to maintain the integrity of the application and works to maximise full use of its functionality.
- Manages organisational reporting.
- Supports the Serious Event Review Committees and reporting to the Clinical Board and Quality, Finance and Risk Committees (QFARC).

Serious Incident Review Committees
Through the Corporate Quality and Patient Safety Department, on behalf of the Clinical Leaders and General Managers, the Committees:

- Promote safety and risk reduction.
- Ensure appropriate review methods are utilised for serious event reviews.
- Monitor incident types, trends, recommendation themes and considers how best to approach improvement (excludes staff incidents).
- Oversee system performance including application maintenance, file management performance, report quality, and adequacy of education and training.
- Oversee monitoring of the implementation of recommendations that arise from:
  - Serious Event Review Reports, Coroner reports; or
  - Health & Disability Commissioner; or
  - Ministry of Health reported system improvements of ACC treatment injury reports; or.
  - Trigger Tools; or
  - Any other sources of incident or near miss data.
  - Monitor timeliness of serious event review reporting, sign off, and implementation of recommendations.
  - Close Serious Event Review Reports (severity assessment code (SAC) 1 and 2) with completed recommendations when approved by General Managers.
  - Ensure the privacy, confidentiality of individual incident data; assure the integrity of data, access management and keep the system secure.
  - Approve incident review templates, tools as well as education and training.
  - Ensure lessons learnt are shared across the organisation.
  - Link to the South Island Safety1st Control Group and Quality and Safety Alliance.

Clinical Boards
Across all areas of CDHB and WCDHB responsibilities (including strategic planning and resource allocation):

1. an improved focus on patient and population health outcomes
2. robust quality improvement systems
3. more effective inter-departmental and inter-organisational functioning
4. a culture of innovation and best practice
5. a skilled and well-supported health workforce.

CEO and Executive Management Teams
The DHB executive management teams will proactively lead strategies, principles, policies and practices that promote optimal outcomes, well designed patient centred systems, and an environment conducive to respect, safety, teamwork and learning.

Quality and Finance Review Committees
On behalf of the respective DHBs', the committees promote safety, and ensure adequate systems are in place to effectively manage incidents, share learnings, and maintain privacy, confidentiality and integrity of individuals' data in the system.

Measurement or Evaluation

Reports demonstrate improvement in regard to key performance indicators, incident trends and improvement actions, including meeting investigation completion timeframes.

The Institute of Healthcare Improvement Global Trigger Tool is used to measure the overall level of harm in our health care organisations. A consistent sample of clinical records are assessed at regular intervals providing a reliable measure on which to judge harm levels over time. Incident reports are provided for 'reported' harm.

Associated Documents

Canterbury and West Coast DHB documents e.g.

- Health Safety and Wellbeing
- Informed consent
- Open disclosure
- Complaints
- ACC Treatment Injury Claims process
- Notification of Serious Wrongdoing
- Consumer, family and whanau feedback
- Fluid and Medication Management
- Adverse Reactions Identification
- Clinical Incident Management Guide
- Safety1st training materials
- Safety1st office procedures
- Canterbury Serious Event Review Committee Terms of Reference
- Contracts with tertiary education providers.

Forms

South Island Regional Safety 1st Reporting Forms

Canterbury DHB Reportable Event Brief (REB)

West Coast DHB Reportable Event Brief (REB)

Electrical Accident Notification Form (available from www.ess.govt.nz)

Form for reporting Adverse Reactions to Medicines, Vaccines and Devices and all Clinical Events for IMMP (available from www.otago.ac.nz/carm or www.medsafe.govt.nz

Definitions

Harm

This refers to any physical or emotional injury to a patient or visitor, or damage to property or the environment. Patient harm is unrelated to the natural course of the patient's illness or underlying conditions, and differs from the expected outcome of the health care provided.

Serious harm is determined by a SAC score of 1 or 2.

Hazard
This is an activity, arrangement, incident or substance that is an actual or potential source of harm, or gradual process condition.

Incident
This is an unplanned or unexpected event resulting in, or having the potential for harm, ill health, damage, loss or disruption to service delivery. This includes being verbally abused by any person (visitor, patient or staff).

Just Culture
A just culture recognises that professionals make mistakes and acknowledges that even competent professionals will develop unhealthy norms (shortcuts, 'routine violations') which need to be addressed. A just approach has zero tolerance for reckless behaviour.

Near Miss
This is an incident which under different circumstances could have caused harm to a consumer but did not, and which is indistinguishable from an adverse event in all but outcome (definition from National Reportable Events Policy 2012).

Open Disclosure
Open disclosure or communication refers to the timely and transparent approach to communicating, engaging with, and supporting consumers and their families (whānau) when things go wrong - refer to the Open Disclosure Policy.

An apology is made and, if an investigation is to take place, those concerned are advised and may be involved, and always receive the report.

Review Methods
Both DHBs' have developed robust methods of review:

1. Serious Event Review (SER)

   This type of review involves a full team of staff (process support, technical expert(s), content expert(s), frontline staff member and possibly a consumer) gathering information about the incident and producing a report. The Canterbury DHB's Serious Event Review report template encompasses key aspects of both of the following recognised methodologies:

   Root Cause Analysis (RCA): A systematic, review where factors that led to an incident are identified in order to establish the contributing factors/hazards/causes. The focus is on systems and processes rather than individuals.

   London Protocol: A process of incident investigation and analysis designed to be a structured process of reflection on incidents providing a 'window on the healthcare system' (Vincent, QSHC 2004).

2. Independent File Review (IFR) – (includes 'clinical review')

   An independent file review is a detailed and thorough review following a patient sustaining significant harm or a near miss event with the potential for significant harm. It uses a similar approach to the SER, although is less resource intense than the SER methodology, in that the review may initially be conducted by two people (may be one

person for Specialist Mental Health only) and then the report approved by a committee.

3. Service Level Review

   A review by senior department staff that are independent from the treating team. The incident is discussed by the multidisciplinary team (MDT) then a nominated person writes a brief report [LINK] which is then agreed by the MDT.

4. Mortality & Morbidity Review - (includes 'facilitated interdepartmental review')

   Mortality and Morbidity Reviews (M&Ms) are a routine, structured forum for the open examination and review of cases involving patient illness or death. The aim is to collectively learn from these events and to improve future patient management and quality of care.

5. Post Falls or Pressure Injury Event Review

   Utilises a specifically developed, concise Post Falls or Pressure Injury Human Factors Assessment Tool [LINK] to review all the relevant factors that may have contributed to the event occurring.

6. Standard Line Manager Review

   A simple process by the line manager of evaluating the details recorded in Safety 1st, gathering additional information if required, identifying contributing factors and implementing and recording any actions taken in Safety 1st.

Severity Assessment Code (SAC)

SAC is a numerical score given to an incident. This is based on the consequence or outcome of the incident and the likelihood that it will recur - refer to the HQSC website.

References

- Health Quality and Safety Commission (HQSC), 2017. *National Adverse Events Reporting Policy: New Zealand Health and Disability Services.* Wellington. Author; http://www.hqsc.govt.nz/our-programmes/reportable-events/national-reportable-events-policy/
- HQSC. 2012 Severity Assessment Criteria tables http://www.hqsc.govt.nz/our-programmes/adverse-events/publications-and-resources/publication/636/
- Health Quality and Safety Commission. *Serious Adverse Events Reports*. Wellington. http://www.hqsc.govt.nz/our-programmes/reportable-events/serious-adverse-events-reports/
- New Zealand Nurses Organisation, 2003. *Incident Reporting (NZNO)*; Wellington; http://www.nzno.org.nz/Portals/0/publications/PUB%20Incident%20reporting.pdf
- Standards New Zealand (2008). *NZS 8134.0:2008 Health and Disability Services (General) Standards.* Wellington; Author; http://www.health.govt.nz/our-work/regulation-health-and-disability-system/certification-healthcare-services/health-and-disability-services-standards
- Taylor-Adams, S and Vincent, C. *Systems Analysis of Clinical Incidents: The London Protocol.* London, United Kingdom: Clinical Safety Research Unit, Imperial College London. Available via http://www.hqsc.govt.nz/our-programmes/reportable-events/publications-and-resources/publication/528/

- Lynn, D. 2008. *Notification of Serious Harm Arising from the Work of Registered Health Professionals*. Department of Labour (now the Ministry of Business, Innovation and Employment); Wellington.

Legislation

- Employment Relations Act 2000
- Health Information Privacy Code 1994
- Public Records Act 1995
- Official Information Act 1992
- Privacy Act 1993

Ara Institute of Canterbury Requirements

When an Ara student or any teaching staff are involved in an incident, the standard Canterbury DHB incident management process is utilised. The appropriate Ara Clinical Liaison Nurse and Canterbury DHB Director of Nursing or delegate (e.g. Duty Nurse Manager after-hours) is notified at the time an incident occurs.

Any records are to be completed with Ara involvement in the process. Tracking events over time can provide useful information for student placement and education.

Summary of Safety1st Support

(Manager includes administrative or clinical leader/ manager or service managers)

Ref	Service		Provided By	Provided To (Users)
Prerequisites				
P1	Orientation and expectations about staff reporting of incidents (local escalation process)	Provide orientation and support to new staff about the incident management policy and local procedures	*Manager or delegate*	All staff new to area
P2	Corporate orientation	Overview of Safety1st and how to submit an incident	*Online programme*	All new staff
P3	Standards for investigation and follow up for improvement	Establish, teach and support the required level of investigation into incidents, action plan and track improvements. This includes data quality and completion	*Divisional Quality Teams*	New managers or investigators
P4	Local clinical governance	Active clinical governance in which incident reporting, issues / themes and improvement actions are discussed/ shared/ planned, and tracked	*Local service*	Clinical leaders managers
A. LOCAL AREA Safety1st SUPPORT				
A1	Request for new Safety1st file manager/GM access	Determine the access need and put in request to Quality Team	*Manager recruiting*	Quality Teams
A2	Resigning file manager access	Notify Safety1st and Quality Team	*Manager recruiting*	Quality Teams
A3	Orientation to investigation requirements and tools to new file managers	Provide orientation and support to new file managers and senior managers	*Manager recruiting*	Divisional Quality Team
A4	Clinical governance	Ensure active clinical governance in which incident reporting, issues / themes and improvement actions are discussed/ shared/ planned, and tracked	*File manager*	Team

Ref	Service		Provided By	Provided To (Users)
B. LOCAL DHB DIVISIONAL Safety1st SUPPORT				
B1	Determine Safety1st file manager requirements	Determine the access rights, widgets and alert requirements of new managers and request to Safety1st	*Divisional Quality Teams*	Safety1st Office
B2	Orientation to investigation requirements and tools	Provide orientation and support to new file managers and senior managers	*Divisional Quality Teams*	File Managers and above
B3	Investigation and data quality	Review and assure the quality of data submitted	*File Manager*	Divisional Quality Team
B4	Investigation and data quality, and closing events	Review and assure the quality of investigation, actions, data submitted then close event	*Divisional Quality Teams*	CDHB
B5	Set up access to required reports for senior managers	Identify required reports and establish access	*Divisional Quality Teams*	File managers and senior managers
B6	Set up of specific reports	Identify required reports and request access	*Divisional Quality Teams*	File managers and senior managers
B7	File Management Training	Hand on training on how to manage a file	*IS Trainers or Divisional Quality Teams*	New File Managers
B8	Request file deletion	For forms that are started but then it is assessed t to that there is no incident report	*File Manager or service based QI staff*	Divisional Quality Team
C. SERVICE DESK Safety1st SUPPORT				
C1	ISG problems	Provide technical support to users for computer and network problems, Escalate software problems to the Safety1st Office and RL6	*Service Desk*	Workforce
D. CDHB & WCDHB Safety1st TEAM SUPPORT				
D1	Set up file manager on the system	Set up a new file manager in the application within 3 days of receiving the written request	*Safety 1st Team*	Manager recruiting
D2	File manager resignation	Archive file managers who have left position	*Safety 1st Team*	CDHB & WCDHB Safety 1st Teams

Ref	Service		Provided By	Provided To (Users)
D3	Set up CDHB & WCDHB reports	Configure reports based on approved operational data definitions Keep a record of definitions etc and a history of changes to reports as per document/ version control	*Safety 1st Team*	CDHB & West Coast Corporate Quality
D4	Provide advice		*Safety 1st Team*	Divisional Quality Managers
D5	Delete Files		*Safety 1st Team*	CDHB & WCDHB Corporate Quality Manager
D6	Training	Provide training objectives, delivery methods and evaluation tools for training	*Safety 1st Team*	CDHB Corporate
D7	Core training materials	Keep up to date and document control training resources	*Safety 1st Team*	CDHB & WCDHB Corporate
D8	Audit system quality	Develop, manage and monitor end to end quality assurance processes	*Safety 1st Team*	CDHB & WCDHB Corporate
E. REGIONAL Safety 1st SUPPORT				
E1	Provide RL6 Software and Updates	RL Solutions / Regional Sys Admin Group	*SI Safety 1st Team*	South Island Region
E2	Provide Infrastructure Hosting Services for RL6	CDHB	*ISG*	South Island Region
E3	Provide Level 3 Centralised Contact point for Technical Liaising with RL Solutions	CDHB	*SI Safety 1st Team*	South Island Region
F. CDHB Safety 1st CHANGE REQUESTS				
F1	Request for changes	Identify the problem to be overcome and the outcome to be achieved	*Divisional Quality Manager*	CDHB & WCDHB Safety1st Team
F2	Clarification of request	Establish problem issue to be solved, clarify if configuration, functionality or training issue	*CDHB Safety1st Team*	Submitting Quality Managers
F3	Change impact and analyses	Analyse changes, suggest options	*SI Safety1st Team*	Director, Quality &Patient Safety

Ref	Service		Provided By	Provided To (Users)
F4	Option endorsement	Confirm option selection and determine if change is to go on regional register	*Quality Managers Meeting*	Regional Safety1st Office
G. SI TEAM CHANGE REQUEST				
G1	Development of system enhancements	Regional User and taxonomy forum	*SI Safety 1st Team*	South Island Region
G2	Approval of system enhancements	Control Group	*SI Safety 1st Team*	South Island Region
G3	Regional Sys Admin Support	Regional Sys Admin Group (Client Key Contacts)	*SI Safety 1st Team*	South Island Region

Information Security Management Policies

Contents

Introduction

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

information, information processing systems and information processing resources.

Purpose

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

Policy

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

Objectives

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

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

Scope

Persons

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

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

Electronic Information

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

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

Information Systems

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

Responsibilities

Overall Responsibility

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

Users

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

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

Partners and Third Parties

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

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

Outsourcing

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

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

Service Level Management

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

Information Sensitivity

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

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

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

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

Ownership of Information

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

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

Monitoring of Information Systems

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

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

Personal Use of Information Systems

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

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

Violations of Policy

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

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

Approved Non-Compliance

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

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

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

Accreditation

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

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

Associated documents

CDHB documents, e.g.

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

Policy statement

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

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

Health Intranet of New Zealand General Security Policy

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

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

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

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

Contents

Purpose

To enable Canterbury District Health Board (CDHB) and West Coast District Health Board (WCDHB) to execute their stewardship role within their legal and regulatory recordkeeping obligations (Public Records Act 2005) in a manner that contributes to engendering public trust and confidence in the integrity of the DHB by establishing the basis for the management of all information, excluding patient information, at or on behalf of CDHB and WCDHB.

Policy Statements

Information Management

The CDHB and WCDHB Corporate Information Management Policy describes the minimum requirements for information creation, maintenance, storage, and protection to deliver the following benefits:

- The right information is available and easily accessible
- Information is complete and available, to support better decision making
- Consistent approach to managing information
- Increased efficiency and productivity
- Risk mitigation by being able to show the process that was followed
- Transparency of decision making and the process followed
- Reduced rework and reinventing the wheel

Information Ownership

All information created or received as part of CDHB and WCDHB activity is the property of CDHB and WCDHB, regardless of physical location, source or medium. Employees, agents, contractors, and volunteers may be delegated stewardship over it and are accountable for its management.

Information created by contractors, suppliers, researchers and students on behalf of or in the conduct of DHB activity is the property of CDHB and WCDHB unless there is an explicit agreement between the parties specifying any exclusions.

Context:

- *This statement is intended to draw a distinction between ownership and stewardship. Information is a DHB resource and is not personally owned by the employees, contractors or agents who create and/or use it.*
- *Ownership of information refers to control of the CDHB's or WCDHB's copy of that information for statutory purposes and does not necessarily imply the exclusive transfer of intellectual property rights.*
- *CDHB and WCDHB will respect the intellectual property rights of other parties and comply with any conditions contained in any licence for information CDHB and WCDHB has to use.*
- *Information created by agents and contractors on behalf of CDHB or WCDHB may continue to be owned by the creator organisation through explicit agreements with the CDHB or WCDHB.*

Information Privacy and Confidentiality

Information that has been defined as confidential must be protected from unauthorised access, use and disclosure. Whether information is confidential depends on the circumstances, and the potential legal, commercial and personal sensitivity implications should all be considered.

Context:

- *The release of information will comply with the principles set out in the Privacy Act 1993, the Public Records Act 2005 and any other legislation requiring the protection of the privacy of individuals.*
- *Official information is to be made available in accordance with the Official Information Act and the principle that the information shall be made available unless there is a good reason for withholding it.*
- *Information that has legal, privacy or commercial sensitivity must be protected from inappropriate use and disclosure. This may include:*
  - *Information, of a personal nature, about individual employees, clients or stakeholders*
  - *Information relating to any legal proceedings in which CDHB or WCDHB is involved*
  - *Information related to any restructure or reorganisation of CDHB or WCDHB*
  - *Information relating to specific products and services provided or proposed for provision including pricing.*
- *Except where legislation precludes making information available, CDHB and WCDHB will make information for which it is the steward available easily and widely to the public, either directly or through private sector distributors. This includes metadata describing CDHB and WCDHB information.*

Information Security

All information and the systems that it resides in, are to be kept secure against unauthorised access, theft, and vandalism to ensure its authenticity and integrity. Greater levels of security will be applied to information agreed to be most important and where loss and unauthorised access would pose the greatest risk to the business (vital records).

Context:

- *Provides for the protection of information, by directing that information must be kept in secure systems and areas.*
- *Provides for the protection of the vital records that are essential to the continued functioning of CDHB and WCDHB.*
- *Specific security measures will be applied to information carried away from the DHB premises.*
- *Information which is accessed remotely will be protected from unauthorised access or use.*

Creation, Receipt, and Management of Information

Every CDHB and WCDHB employee, agent, contractor, student and volunteer is to capture information to document all activities and transactions. Information should be stored in a way that enables efficient retrieval (including appropriate electronic and hard copy filing). This information must be captured in the CDHB's and WCDHB's approved information system using an approved process with appropriate contextual information.

Context:

- *This section is concerned with providing CDHB and WCDHB with a history of its knowledge and activities, to support good business practice, promote efficiency, and support risk management.*
- *Information must be preserved and managed in a way that they are readily accessible if necessary.*
- *Information can provide unique evidence of events and decisions, which is hard to reconstruct or replace. It therefore protects CDHB and WCDHB's interests and the interests of its clients.*
- *Information captured must be relevant, accurate and fit for purpose for the CDHB and WCDHB and be a true representation of the activity.*

Retention and Disposal

Information must be retained and properly preserved in an accessible format for as long as needed to meet business needs and requirements of legislation. Information deemed to be of continuing value will be identified and retained in a useable form for the appropriate length of time. Disposal of information must be authorised and managed in accordance with security and environmental requirements.

Context:

- *This section is concerned with ensuring accountabilities and legislative requirements regarding the retention and disposal of information are met.*
- *Information must be kept while of use to the DHB or as governed by legislation. Equally, information should not be retained longer than is necessary.*

- *Information must be protected, maintained, accessible and useable for the entirety of its retention period.*
- *Destruction of information of all media types will be irreversible, secure and documented.*
- *Information assessed as being of long term value must be transferred to appropriate archival storage once it becomes inactive or has been in existence for 25 years or more.*
- *To deal with obsolescence, electronic information of long term value may need to be migrated to a format more acceptable for long term preservation.*

Scope

This policy applies to all information, excluding patient information, which is generated or received as part of any CDHB or WCDHB activity, regardless of format.

Separate policies regarding patient information can be accessed under the Legal and Quality section of manuals, via the intranet (CDHB) or via the intranet (WCDHB).

The information management policy applies equally to all CDHB and WCDHB employees (including full time, part time, casual and temporary), agents, contractors, students, visiting health professionals and volunteers.

Definitions

What information is covered by this policy?

Information is any knowledge, facts, or data produced or received that relates to CDHB and WCDHB activity. It does not include patient information.

The Public Records Act 2005 defines information as: “information, whether in its original form or otherwise, including … a document, a signature, a seal, text, images, sound, speech or data compiled, recorded, or stored … in written form on any material, or on film, negative, tape or any other medium so as to be capable of being reproduced, or by means of any recording device, or process, computer, or other electronic device or process.”

This means that information includes hard copy files, photographs, electronic documents (such as those created in Word, Excel, PowerPoint, FrontPage, Visio and Project), videos and social media.

Examples of information are:

- Emails used for communication
- Templates and forms used to create documents
- Drawings and images
- All documents that have been created by or are related to CDHB or WCDHB.

Further definitions

Access	The right, opportunity or means of finding, using or retrieving information.
Agents	Independent entity that agrees to provide personnel, and/or services that meet or exceed stated requirements or specifications, at a mutually agreed upon price and within a specified timeframe.
Copyright	A property right primarily concerned with publication of original material.
Destruction	The process of eliminating, destroying or deleting records that prevents them from being reconstructed.
Disposal	The removal of information from the information management system.
Document	A piece of written information whether in physical or electronic format including, but not limited to: emails, faxes, letters, reports, memos, hand-written notes, spreadsheets.
Owner	Information must be under the care and management of an owner to determine access and storage requirements. The owner is also referred to as the steward.
Format	The way in which data or information is captured or rendered. Formats may include but are not limited to: text, drawing, sound recording, still image, or moving image.
Integrity	The integrity of information refers to its being complete, unaltered, and protected against unauthorised alteration. Any authorised annotation, addition or deletion of information must be explicitly indicated and traceable to uphold the integrity of information.
Location	The location of electronic information on the server, or within the document management system, or the physical location of a hard copy item.
Media	Materials that hold data in any form or that allow data to pass through them, including paper, transparencies, multipart forms, hard, floppy and optical disks, magnetic tape, wire, cable and fibre.
Metadata	Defined as "data about data" it's used to describe information and documents (digital or otherwise), its relationships with entities, and how the document has been and should be treated over time. Metadata allows users to locate and evaluate documents without each person having to discover it anew with every use.
Preservation	Processes and operations involved in ensuring the technical and intellectual survival of authentic information through time.
Disposal Authority	The authority document that controls how long information is retained or disposed of and the time frame within which this must occur.
Stewardship	Information must be under the care and management of a steward or custodian to determine access and storage requirements. The steward is also referred to as the business owner.
Vital records	Vital records are records that are essential for the ongoing business of the DHB, without which it could not continue to function effectively.

Roles and Responsibilities

All Staff	➲ Following the Information Management Policy and Procedures.
Managers	➲ Ensure that business rules and processes in your area of responsibility include the capture of information into approved systems, including email. ➲ Ensure that staff follow the processes for information creation, capture, receipt, retrieval, storage, and disposal. ➲ Manage approval of external requests for use of or access to information of which you are considered to be owner. ➲ Ensure that personal or confidential information within the activities in your area can be identified and protected from unauthorised access. ➲ Ensure any policy or procedure documents you create include record keeping requirements. ➲ Ensure that any staff you manage adhere to information retention and disposal requirements. ➲ Approve the disposal (transfer to archival storage or destruction) of information in your area.
Information Management staff	➲ Work with managers and staff to ensure information and capture management supports current business processes. ➲ Monitor that CDHB and WCDHB are meeting the Records Management Standard requirements and comply with this policy. ➲ Identify if there is private or confidential information within the data and information sets and appropriate levels of security are applied. Provide direction to managers on appropriate access and protection for this information. ➲ Work with Information Governance to identify high value and high priority information. ➲ Work with ISG to ensure retention and disposal actions are applied appropriately to electronic information. ➲ Oversee the retention and disposal of CDHB and WCDHB information as outlined in the approved DHB General Disposal Authority.
ISG	➲ Provide appropriate tools and systems for the creation and capture of information. ➲ Ensure systems are not able to be accessed by external parties unless there is explicit permission for this by the owner. ➲ Ensure that tools and systems used for managing information have appropriate mechanisms for managing access permissions and restrictions. ➲ Provide tools and support for the monitoring and measurement of information access. ➲ Provide information system disaster recovery plans, tools, procedures and training. ➲ Provide retention and disposal tools.

Executive Sponsor	➲ Ensures that CDHB has in place Information Management Policy that aligns with the CDHB's and WCDHB's strategic goals and objectives ➲ Ensures the CDHB's and WCDHB's organisational structure supports the expectations outlined in the Information Management Policy
Corporate Legal and Corporate Support	➲ Supports that appropriate tools and systems are in place to enable information management to meet the standards and relevant legislation.
Transalpine Information Manager	➲ Ensure appropriate repositories are available for the management of CDHB and WCDHB information and work with the relevant staff. ➲ Initiate remedial action if information accessibility is compromised. ➲ Identify vital records and ensure that they remain accessible. ➲ Ensure that retention and disposal of information is executed regularly ➲ Measure and monitor the transfer of information to archival storage and the ongoing accessibility of that information.
Contract Managers	➲ Ensure that a statement on information ownership is included in appropriate contracts. ➲ Ensure that information created by contractors is captured in a CDHB or WCDHB approved system.
Privacy Officer	➲ Consider and make recommendations on requests for personal information.

Associated Documents

All documents will cover specific information management requirements.

Measurement or Evaluation

This policy will be monitored regularly for adherence and reviewed at least every 3 years to ensure that it remains relevant to the DHB's business aims and requirements.

Employees' adherence to the policy and procedures will be monitored on an on-going basis through self-assessment and as part of the regular performance review process.

Because the policy covers the requirements covered in the Public Records Act, the intent of this policy will be officially measured through an audit by Archives New Zealand.

References

Related legislation and policies (for Policy Web)

- Public Records Act 2005
- DHB General Disposal Authority
- Copyright Act 1994
- Electronic Transactions Act 2002
- Employment Relations Act 2000
- Health and Safety at Work Act 2015
- Holidays Act 2003
- Ombudsman Act 1975
- Privacy Act 1993
- Financial Reporting Act 2013
- Financial Transactions Reporting Act 1996
- Goods and Services Tax Act 1985
- Contract and Commercial Law Act 2017
- Income Tax Act 2004
- Public Finance Act 1989
- Official Information Act 1982
- New Zealand Public Health and Disability Act 2000
- Health & Disability Commissioner Regulation 1996
- Health Act 1956
- Health and Disability Services Standards 8134.1:2008

Note: This is not an exhaustive list.

Disclosure of Adverse Patient Events Procedure

Purpose

This Procedure is performed as a means of improving the quality of care delivered to West Coast District Health Board (WCDHB) patients/ consumers and maximise patient/ consumer safety, through the identification and analysis in a timely manner of those patient events that are adverse.

Applicability

This Procedure is to be followed by WCDHB Clinical staff members.

Definitions

For the purposes of this Procedure:

Adverse Event is taken to mean an unexpected, unintended occurrence that results in injury to the patient or has the potential for causing injury. Examples include events that require additional treatment, increased monitoring, delay in discharge or transfer to another healthcare facility.

Serious Incident is defined as an incident which has an adverse outcome and includes:

- client/ patient suicide
- deliberate self-harm/ attempted suicide by a client/ patient
- physical violence resulting in injury to a client/ patient/ staff member
- admission of a client/ patient following unsuccessful treatment by another health provider
- hospital-incurred trauma/injury of a client/patient
- client/patient AWOL
- sudden death of a client/patient
- accident/incident involving a staff member that resulted in serious harm or death,

  OR

  Any other accident/ incident that in the opinion of the Chief Executive Officer or General Manager needs to be classified as a serious incident

Roles and Responsibilities

For the purposes of this Procedure:

The ***Chief Executive Officer*** is required to:

- oversee all aspects of this Procedure.

Staff Members are required to:

- ensure they abide by the requirements of this Procedure.

Resources Required

- Safety1st Electronic Reporting System

Process

1.00 Open disclosure of adverse events

- contributes to the foundation of a successful health professional-patient relationship by ensuring that trust between the health professional and patient is not compromised;
- is a right of a patient under the Code of Health and Disability Services Consumers' Rights;
- is part of the move towards increased accountability from health professionals;
- is necessary for the informed consent process, especially when the harm results in the need for further treatment or care;
- contributes to public awareness, information, and education about the reality of medical treatment;
- provides an environment that enables health professionals to learn from others' mistakes in an educational manner because harm can be discussed openly;
- is not about attributing blame.

1.01 Disclosure to the patient and/or family/ whanau/ caregiver should generally be made when any adverse patient event has occurred. In some situations, consideration should be given to discussing adverse events that do not result in patient injury (i.e. “near misses”). The decision to disclose will depend on the specific circumstances of the event.

1.02 Disclosure should take place at the right time, when the patient is medically stable enough to absorb the information, and in the right setting. In situations where the patient has suffered permanent injury or death, information should be provided to the patient’s family/ whanau/ caregiver or legal representative in a timely and considerate manner. Typically, disclosure should take place within 24 hours after the event has occurred or is discovered.

1.03 In most cases, the health professional with overall responsibility for the patient’s care, i.e., the Senior Medical Officer (SMO), should handle the disclosure of information as well as subsequent discussions with the patient and/or family. In some situations, however, other health professionals may be more appropriate to disclose the event, such as relevant General Manager or other health professionals who has the most information about the event and/or has an existing relationship with the patient and family/ whanau/ caregiver

1.04 At least one other staff member (either clinical or management) should be present at the initial disclosure discussion or at subsequent planned discussions with the patient and/or family/ whanau/ caregiver.

1.05 When having the initial disclosure discussion with the patient and/or family/ whanau/ caregiver, it is important for staff members to acknowledge that the adverse event has

occurred and to make some expression of personal regret and apology for the event. Patients and family/ whanau/ caregivers often appreciate an expression of regret and empathy. Saying "I'm sorry" will help to strengthen, rather than undermine, the health professional-patient relationship.

1.06 The next step is to describe in a truthful and compassionate manner the following:

- The nature of the event as it is understood at the time of the discussion;
- The time, place and circumstances of the event as it is understood at the time of the discussion;
- The known, definite consequences of the event for the patient, as well as any anticipated or potential consequences;
- The corrective actions taken in response to the event which may include ongoing communication with the patient and family/ whanau/ caregivers as is necessary;
- Identify who will be managing ongoing care of the patient;
- Identify who will manage ongoing communication with the patient and/or family/ whanau/ caregiver, including names and phone numbers of individuals at the relevant WCDHB facility to whom the patient and family/ whanau/ caregiver may address questions, complaints or concerns.

1.07 As soon as is practical after the adverse event has occurred; it is to be recorded using the WCDHB Safety1st electronic system.

1.08 The patient's clinical record should also contain a complete, accurate and factual record of pertinent clinical information related to the event and should be completed in a timely manner. The documentation should include:

- Objective details of the event, including date, time and place
- The patient's condition immediately before the time of the event
- Medical intervention and patient response
- Notification of other health professionals
- Additionally, documentation outlining the disclosure discussion with the patient and/or family should include:
- Time, date and place of discussion
- Names and relationships of those present at the discussion
- Documentation of discussion of the event
- Documentation that additional information has been shared with the patient/ family/ whanau/ caregiver or legal representative, if appropriate
- Documentation of any follow-up conversations

1.09 When documenting the adverse event, staff members are not to assign blame, make assumptions or draw conclusions about the event. Staff members are also not to use the patient's clinical record to make complaints about staffing, facility or department issues. This information is to be recorded using the WCDHB Safety1st Electronic System.

1.10 Harm to patients is rarely the result of deliberate negligence or incompetence and the health professionals involved may find the experience stressful and difficult. It is important that these health professionals have access to support, which is available via the internal WCDHB Peer Support Programme, and externally via the Employee Assistance Programme (EAPS). The WCDHB Wellbeing and Occupational Health and Safety Advisor should be contracted for information regarding these processes.

Precautions and Considerations

- Disclosure to the patient and/or family/ whanau/ caregiver should generally be made when any adverse patient event has occurred
- When having the initial disclosure discussion with the patient and/or family/ whanau/ caregiver, it is important for staff members to acknowledge that the adverse event has occurred and to make some expression of personal regret and apology for the event
- Disclosure should take place at the right time, when the patient is medically stable enough to absorb the information, and in the right setting
- It is important that these health professionals have access to support

References

- Code of Health and Disability Services Consumers' Rights (1996)

APPENDIX 5

Access Control (ICT) Policy

Purpose

To exercise sufficient control over information to prevent unauthorised access.

The District Health Board (DHB) owns and operates computer information systems provided for use by employees in support of organisational activities.

Access controls help stop unauthorised information access, including health information, ensuring it remains confidential. Access to information systems is a tool of employment for which access is granted during a term of employment or engagement, and must be removed as soon access is no longer required.

The purpose of this policy document is to state requirements for the creation and removal of access permissions to DHB information systems.

Policy

All users must be authorised and must only view and process the information they are entitled to and have a need to access.

Scope

This policy outlines the permitted and effective access to District Health Board and regional computer information systems and electronic information by users. Guidance on appropriate Information Systems (IS) account management and strong password management practices is provided to ensure systems are protected from unauthorised access, disclosure, modification, or use.

This policy applies to all staff and all individuals engaged or contracted for services to do work for the DHB and who are required to access DHB and/or regional information systems.

Definitions

CDO: Chief Digital Officer

DHB: District Health Board. Refers to both Canterbury District Health Board and West Coast District Health Board

ICT: Information and Communications Technology

ISG: Information Systems Group

IS: Information Systems

PHO: Primary Health Organisation

W/CDHB: West Coast or Canterbury Disctrict Health Boards

Roles and responsibilities

The five information systems roles in the DHB are:

1. user – DHB staff member, with sufficient access rights to perform their role.
2. non-DHB staff – Third party organisation or individual who requires access to DHB information systems e.g. student nurse, PHO, private specialist etc.
3. vendor – third party company or individual engaged by the DHB to provide or support services e.g. Ricoh.
4. managers in departments providing information services – including but not limited to Information Services Group, Maintenance & Engineering, Clinical Engineering, Radiology, Labs, Oncology and Decision Support.
5. ICT administrator – DHB staff member with elevated rights to enable them to provide/support information services.

Any person with access to DHB information systems MUST comply with all USER policies in this document and any confidentiality and disclosure agreements they may be asked to sign.

ICT administrators, vendors, and non-staff may have additional requirements placed on them, which will be made clear to them prior to access being granted.

Associated documents

W/CDHB documents:

- Code of Conduct
- Information Management Policy
- Responsibility for Information Security Policy
- Mobile Devices and Working Outside the Office Policy
- User Policy
- Third Party and Supplier Policy

Non-Compliance

Protection of our information systems and the information stored on them is of critical importance to the DHB. Providing access to these systems and information through disclosure of passwords to others, or by inappropriate password selection and use, may be grounds for loss of computing privileges, and for misconduct and disciplinary procedures, in accordance with the DHB Code of Conduct.

In the event that an account or password is suspected to have been compromised, the incident must be reported to ISG Service Desk immediately. All passwords are to be changed immediately.

Passwords

Passwords for individual accounts are not to be shared with others. In exceptional cases, with the approval of the CDO, passwords may be shared with named individuals in specific roles; a register of approvals is to be kept by ISG.

For standard user and non-staff accounts without elevated privileges the DHB is implementing increased complexity of passwords but removing the need to change the password unless it is believed to be compromised. Information system mechanisms are to be in place to ensure users do not choose simple passwords and that chosen passwords are not commonly available on lists of hacked internet passwords.

Passwords for administrator and vendor accounts with elevated privileges are required to be changed at least once every 3 months.

Access Management

It is the responsibility of Authorising Managers (registered with People & Capability) to ensure that their staff, vendors, and non-staff have appropriate access when they start working for the DHB and if the change jobs, roles, and/or locations.

ISG is to be advised of changes to roles, jobs, and locations as follows:

- for Canterbury staff via the automated form on the Service Desk Portal
- for West Coast staff via the iAccess tool.
- for non-staff / vendors via the ISG forms on the DHB Intranet

Authorising managers are to approve access on a 'least rights' model where only the access needed to perform a role is requested. If authorising managers are unsure or do not understand what they are granting access to, then they should contact the ISG Service Desk.

Note:

- that People & Capability, Security, and Information Systems forms and processes are not yet fully linked and so informing one department does not always currently inform the others. Staff should check whether other departments need to be advised separately.

Network or application accounts that are unused for 90 days are to be automatically locked where this is possible.

Old Accounts

Accounts that have been inactive for a minimum period must be disabled. Disabling an account means that the person cannot log in and therefore does not have access to any electronic information such as e-mail or corporate documents. The information owned by that account is still available to the manager or other authorised people.

Logon accounts that have been disabled for a minimum period must be removed. Removing an account means that all access to the account is completely removed, along with all information owned by that account, including directories, files and email messages. Directories and files stored in shared areas will not be deleted.

- People and Capability and/or the manager of the area associated with an information system account that is to be removed may request access to information owned by the account before it is removed.
- The divisional People and Capability department and/or the manager of the area associated with an IS account that is to be removed is responsible for ensuring any information associated with the account (including directories, files and electronic mail messages) is saved or moved if necessary before it is removed.

- Assistance with saving information may be requested through the ISG Service Desk if not specifically included in the account removal process.

User Responsibilities

Act Responsibly

Read, review and understand obligations under the access control policy.

Do not leave the computer unlocked while unattended. Terminate any active sessions, lock the screen, log off or disconnected when finished.

Take responsibility for all activities and privileged information that is accessed under your logon.

Ensure all access is related to your duties.

Report any security breach.

Comply with DHB policies relating to the use of mobile devices and working outside the office.

Ensure any account used for handling and management of patient-identifiable information, regardless of the device used, is restricted to that purpose. For example: coupling or automated linking of those user accounts to social media sites on the internet is not acceptable.

If users have more than one account due to having two or more roles; then they must use the appropriate account for the role they are filling at any particular time.

Authorised Use

DHB information systems may only be used for the purpose intended and by authorised personnel.

DHB information systems must not be used for non-DHB purposes including soliciting business, selling products or services, or otherwise engaging in commercial activities, other than those expressly permitted by Executive Management Team Members or General Managers.

Users of a DHB information system may not gain unauthorised access to any other DHB or regional information system, or in any way disclose, damage, alter or disrupt the information on it, or the operation of the system.

Users are prohibited from exploiting vulnerabilities or deficiencies in information security, capturing or otherwise obtaining passwords, or the use of any other access mechanism, which could permit unauthorised access.

Failure to comply with these conditions will result in disciplinary action being taken.

Passwords

Follow good practice in the selection and use of passwords.

DHB passwords must be chosen carefully so that they are easy for you to remember but hard for others to guess, so they don't have to be written down.

DHB passwords must be changed if you think there's even a chance someone might know your password.

DHB passwords must be protected. You are responsible for all actions carried out under your computer user-ID/ password. You must therefore not disclose your password to anyone, including your manager or people claiming to be from Information Services Group or the Service Desk.

DHB passwords are not to be written down unless they are stored in a sealed envelope in a locked drawer/cabinet and periodically checked that they have not been accessed without your knowledge.

DHB passwords are not to be stored in an electronic password safe unless the application used has been approved by the ISG Risk and Security Manager.

You must not use the same passwords for personal and work related purposes.

You must not use common passwords or previously used passwords for your DHB passwords.

You must not use information easily obtained or known about you as your DHB passwords.

Desk and screen policy for sensitive or confidential information e.g. MEDICAL-IN-CONFIDENCE

The DHB has a 'clear desk and screen' policy to protect paper and information on computer displays being seen by those who should not have access to the information.

- Screens where sensitive/confidential information may be displayed must not be easily visible to patients/public.
- Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.
- Computer workstations must be locked when workspace is unoccupied.
- Restricted or Sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied, and at the end of the work day.
- File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.
- Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.
- Laptops and portable computing devices in publicly accessible areas without suitable manual or electronic access control measures must, where possible, be either locked with a locking cable or locked away in a drawer.
- Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.
- Printouts containing Restricted or Sensitive information should be immediately removed from the printer, where printing on demand functions are not available (such as follow-me).
- Upon disposal Restricted and/or Sensitive documents should be shredded in the official locked secure destruction and recycling bins.
- Whiteboards containing Restricted and/or Sensitive information should be erased.
- Mass storage devices such as CDROM, DVD or USB drives which have sensitive or confidential information must be secured in a locked drawer.

Non-DHB Staff and Responsibilities

Non-DHB staff responsibilities will be highlighted in the request forms that they are required to sign.

- Non-DHB Staff accounts are to be easily identifiable as non-DHB staff accounts, but also be individually named, and permissions limited to the minimum permissions required.
- Every 12 months, or less if appropriate, the accounts are to expire and not be re-enabled without a request from the non-DHB organisation.
- ISG is to notify non-DHB organisations one month prior to account expiry.

Vendor Accounts and Responsibilities

Vendor responsibilities will be highlighted in the request forms that vendors are required to sign.

- Vendor accounts are to be easily identified as vendor accounts but also be individually named, and permissions limited to the minimum permissions required.
- If access is required for a project then the accounts must expire at the end of the project.
- Vendor accounts will be enabled for specific activities and then locked unless an exception has been granted by the CDO.
- Every 12 months the accounts are to expire and not be re-enabled without a request from the CDO.

Responsibilities for Departments Providing Information Services

Process and Audit

Ensure there is segregation of access control administration roles so the same person is not performing multiple roles – e.g. request, authorisation, and administration.

Ensure relevant contractual and legislative obligations are met for the access to data and services such as privacy requirements.

Regularly review access log audit reports, especially for unsuccessful access requests of accounts/applications and the activity of privileged accounts.

Establish a process that ensures all granted access permissions are appropriate, documented and traceable, based on the profile of the role and the user's requirement for access to confidential information.

Ensure that, along with terms and conditions of employment (including contractors), there is a mechanism to ensure users sign an agreement that covers information confidentiality and disclosure.

Process and Audit Standards

Undertake an audit or review of user access to all information systems, including external/remote access at least every 12-months. Staff accounts should be reconciled against current Payroll records.

Establish a user account creation and access granting process that is documented and traceable.

In particular the process:

- must list the:
    - information systems to be accessed
    - specific access rights required
- must be approved by:
    - the information system or application owner
- should:
    - enable access rights to be provided and revoked at short notice, to support the requirements of locums and contractors for short-term temporary access
- requires a:
    - statement signed by the user indicating they understand and accept the conditions of access (see also Confidentiality Statements)
    - formal record of the access request and authorisation to be kept
    - separate authorisation process to permit management of systems/information above, that required for a standard user authorisation.

Establish a process so that all employees and contractors sign a security policy responsibility agreement covering information confidentiality and disclosure.

Administrator Responsibilities

Overall Principles

Access must only be granted based on the minimum rights required to perform the role.

The approver of rights must understand what they are granting access to, and must have the authority to grant that access. If a manager wishes to delegate their approval rights, this delegation must be registered with the ISG Service Desk

Password Requirements

Users must be able to select and change their own passwords and include a confirmation procedure to avoid input errors.

Passwords across all applications must conform to a required complexity level based on the risk profile of the users and the information they have access to.

Password complexity for privileged accounts (ICT administrator access) must be equal to or exceed the password complexity required by standard users.

Password changes must be enforced at regular intervals for privileged accounts. Password changes for standard accounts do not have to be regularly enforced, providing there is a control mechanism approved by the CDO to manage this risk.

Previous user passwords may not be reused for a minimum period of time.

User accounts must be automatically locked after a fixed number of incorrect login attempts.

Passwords must be stored and transmitted in a secure encrypted non-reversible format.

When issuing account information for users, mechanisms to adequately protect the transmission of this information must be taken. Passwords must not be communicated to users via unencrypted emails. Login names and password information can be provided over the phone once the identity of the recipient has been established

Administrator Accounts and Passwords

Administrator passwords must be changed every 3 months.

Administrator accounts that have been inactive for 3 months or longer must be disabled. Access must only be granted based on the minimum rights required to perform the role.

Shared Accounts

Generic user-IDs, group-IDs and shared user-IDs should not be used and must not be used to modify patient or other IN-CONFIDENCE information, unless there is another mechanism to identify the individual who made the change.

Creation and use of shared accounts requires the approval of the Transalpine Risk and Security Manager and, as deemed necessary, senior management / clinical approval.

New Staff, Departures and Transfers

Immediately disable logon accounts of staff who have left the employ of the DHB. This includes all application accounts, not just those associated with the user's primary logon credentials.

Ensure a security policy responsibility agreement has been signed by all employees and contractors before granting access.

Follow a process that ensures all granted access permissions are appropriate, documented and traceable.

Access rights for users who have changed role(s) within the DHB must be modified to reflect the new person's role(s).

Access rights for users who have left the employ of the DHB must be immediately revoked.

Personal user account login IDs used by those previously engaged by the DHB are not to be used by new people with similar names.

Non-Staff Accounts

Contractor and other non-staff accounts may be granted temporary access rights for a fixed period only and those accounts must expire at the end of that period.

Contractor and other non-staff accounts must be separately identified from internal staff accounts to enable easier identification and management.

Privileged Accounts

There is a separate, documented authorisation process to permit Administrator level access.

System Settings

Enable multi-factor authentication for access from untrusted networks (e.g. Internet) depending on the level of harm that could result from that system being compromised.

Minimise access times to high-risk systems to reduce the window of opportunity for unauthorised access.

Do not show previous logon names or identifiers until after logon is successful.

Where possible, configure systems to display date and time the user last logged in to assist in identifying unauthorised use of their account.

Automatically close down or terminate a session after a fixed period of user inactivity or provide a locked screensaver option where the user must re-authenticate to unlock the system. Users must not be permitted to disable the locking mechanism.

There is a separate, documented authorisation process to permit Administrator level access.

Ensure any wireless access points providing access to the DHB network are secured and only trusted devices or trusted users can gain access to internal networks via wireless

Responsible Use

Ensure that all privileged user accounts (e.g. administrator rights) are only used for the special activities requiring their use, and not for day-to-day activities or to bypass formal process and controls.

Measurement or evaluation

Compliance with this policy will be measured by audits on an irregular basis.

Policy Owner	Chief Digital Officer, CDHB and WCDHB
Policy Authoriser	Chief Medical Officer, CDHB Chief Medical Officer, WCDHB
Date of Authorisation	(CDHB) (WCDHB)

Incident Handling Policy

Contents

Policy

Incident and problem handling procedures must cover all Canterbury DHB information systems and processing facilities.

Purpose

This document provides general procedures for dealing with information security incidents. It is designed to provide Canterbury DHB personnel with guidelines on what to do if they discover, or are notified of a security incident.

Objectives

The objectives of incident handling are to:

- Limit immediate impact of incident.
- Determine how the incident occurred and by whom.
- Assess impact and damage.
- Recover from the incident.
- Avoid further occurrences of the incident.
- Update policies and procedures as required.
- Provide means for documenting and reporting incidents.

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

Printed copies may not reflect the most recent updates.

Scope/Audience

Canterbury DHB personnel in the event that they discover, or are notified of a security incident.

Definitions

Incidents

The term 'incident' in this document refers to any event which causes, or may cause an interruption to, or a reduction in, the quality of a service. (ITIL definition). Security Incidents are a specific type of incident and may arise from deliberate or accidental activity and can often lead to or result in serious damage or compromise if left unattended. Examples include:

- Unauthorised use of another user's logon/ user-ID.
- Misuse of an application or system
- Access to web sites not commensurate with Canterbury DHB policy.
- Malicious code such as viruses, worms and Trojans.
- Denial of service via a system crash, saturation of network bandwidth, etc.
- System intrusion or hacking/cracking.
- Information theft, loss of confidentiality, data manipulation
- Exploitation of software vulnerabilities.
- Repeated unsuccessful logon attempts, network access, firewall attacks.

Incident handling has a close tie-in with Problem Management, Change Management, Service Continuity Management and other ITIL methodologies.

Areas of Responsibility

Since information security incidents vary in nature and impact, different people will be involved in different incidents, and at varying stages throughout the incident.

Involved parties may be:

- Information Security Manager or CIO – co-ordination and documentation of incident, management escalation and follow-up action.
- Computer and system Users - reporting of incidents or suspected incidents.

- ISG Service Desk – logging details of incidents, invoking Incident Handling procedures, communication with users.
- Information Services staff - investigation of incidents, recovery, and escalation.
- Disaster Recovery Committee – full responsibility for escalated incidents in accordance with DR guidelines.
- Human Resources department – employee counselling and disciplinary action.
- Security Advisor – all aspects of physical and personnel security.
- Legal and Privacy Officers – investigation into release of patient or company confidential information.

Important Considerations

An information security incident may occur at any time of the day or night. Timely investigation of incidents and escalation to management is of paramount importance.

There will at times be conflict between thoroughly investigating and analysing an incident, and restoring service when the incident has resulted in a system or network down situation. In all instances the decision as to which takes precedence must be made Canterbury DHB management and/or the Disaster Recovery Committee. If in doubt it is better to continue with the investigation unless patient safety is threatened by not immediately restoring service.

General Procedures

These steps should be followed for each security incident. However the relevance and importance attached to the steps will vary from incident to incident.

- **Preparation** – knowing in advance how to respond to an incident. Monitoring of alerts, vulnerabilities and malicious software.
- **Discovery/ notification of an incident, a suspected incident, or threat of an incident** – reporting, logging and prioritising incidents, eg:

Priority	Definition	Examples
High	Incident where impact is severe. Systems or network are down. Data is lost, corrupted or compromised (stolen)	Widespread malicious code attacks. Major applications unavailable. System/administrator user-IDs compromised. Theft of Canterbury DHB or patient information.
Medium	Significant impact on users, systems, network and data Potential to have a severe impact if left unattended.	Localised malicious code attacks. Departmental systems unavailable. Apparent change of password without user knowledge. Visit to inappropriate web site.
Low	Incidents that have minimal impact on users, systems, network or data Potential for a significant or severe impact if left unattended	Isolated virus infections (single PC) Firewall probing Software vulnerability alert Theft of a PC/ laptop (could be high priority depending of the data contained thereon)

- **Identification and Analysis** – confirmation of the incident and the nature of it. It is important that at an early stage a snapshot of all available information is taken – this includes copies of all relevant logs, history files, cache buffers, screen prints, audit trails, etc in both soft and hard copy. All other available evidence must also be preserved.
- **Containment** - steps to limit the scope and magnitude of an incident. This will involve determining the best course of action, looking at alternatives and options available.
- **Assess Impact and Damage** - involves a more detailed assessment of the effects of the incident – what the impact has been to date, what the impact currently is, and what it potentially might be.
- **Eradication** - a detailed step involving removal of the cause of the incident. It is essential to avoid further exploitation of any vulnerability and prevent re-infection by malicious code.

- **Recovery** – if workarounds or temporary fixes have been put in place, system recovery back to normal operating status must now occur.
- **Follow-up** - includes:
  - Post incident debrief
  - Root cause analysis / lessons to be learned
  - Full report on the incident including collation of logs and documentation
  - Changes to processes, policies and procedures where required.
- **Escalation** – escalation must be considered at every step, eg.
  - High priority incidents must result in the convening of the Information Services Disaster Recovery Team.
  - Communication to system users may be required.
  - Canterbury DHB executive management (including the Communications Group) may need to be informed.

Reporting

It is important at each step in the process to ensure that all details are documented. This assists staff from forgetting things that were done in the heat of the moment, and provides the basis for later phases, i.e. eradication, recovery , follow-up, and for the final documentation and reporting.

Details to be gathered include:

- Date and time - of each action and response
- How and when was the incident reported/ identified?
- Full contact information of person reporting the incident – name, department, phone, email
- Location of incident
- Description of incident
- What was compromised or damaged (eg. equipment, information, policies)?
- Is this a confidential or sensitive incident?
- Does it appear malicious, intentional or accidental?
- Suspected perpetrator or source of incident
- Details of actions and responses taken at each phase – ie. discovery, identification, containment, impact, eradication, recovery, follow- up (don't forget dates and times).
- Who took the actions

- What were the escalation paths
- Any involvement of or actions by parties external to ISG (Canterbury DHB, 3rd party)

Associated documents

Incident Handling Procedure

Policy statement

Incident and problem handling procedures must cover all Canterbury DHB information systems and processing facilities.

The objectives of incident handling are to:

- Limit immediate impact of incident.
- Determine how the incident occurred and by whom.
- Assess impact and damage.
- Recover from the incident.
- Avoid further occurrences of the incident.
- Update policies and procedures as required.
- Provide means for documenting and reporting incidents.

Policy Owner	Chief Information Officer
Policy Authoriser	Chief Medical Officer
Date of Authorisation	30 August 2015