POLICY ACCESS TO NMDHB's ELECTRONIC INFORMATION SYSTEMS

Policy statement

Nelson Marlborough District Health Board (NMDHB) undertakes to ensure compliance with privacy obligations towards patient information as well as any other business information of a sensitive nature.

Principles

- Users will only access information in the system to carry out the tasks and responsibilities pertinent to their staff role. In other words, information is not to be accessed or used outside the scope of what is required to perform their job.
- Access levels to applications are related to roles, not individuals.
- Temporary User IDs will be given to temporary or locum staff and these will expire at the end of their employment period.
- No sensitive information should be stored on an unsecured local storage device (such as hard disk, floppy disk, CD/DVD, USB drive or portable computer).
- All users are required to sign the Access Agreement (contained in this policy) which makes clear the users's responsibilities for using information systems. The signed form will be stored in the users's HR file
- Third party health care providers need to sign the Access Deed

Scope

This policy covers all electronic access by NMDHB staff, contractors and authorised external users (anyone assigned access to NMDHB information systems) and includes all applications, including those which allow access to patient identifiable health information (e.g. Orion Concerto, Ora*Care).

Definitions

PERC	Paper and Electronic Records Committee
EMR	Electronic Medical Record
Sensitive information	Information that must be protected because it might cause damage to someone or something if revealed to persons not entitled to it. This includes personal and confidential information.

Procedures

General

- A user ID will only ever be assigned to one person.
- Temporary user IDs are issued for the employment period with a maximum period of one year
- Security levels within applications are achieved by creating groups corresponding to common roles and responsibilities. Those groups will be assigned access rights which, by delegated authority, deemed appropriate for that group.
- Users are required to access the systems by logging on with their ID which identifies who they are and a password, which will authenticate that they are who they say they are.

Granting access

- Manager to determine access level appropriate for the role.
- Assignment of rights to individual appointed to this role.
- Temporary and locum staff to receive temporary IDs.

Changing access	If an individual is appointed to a different role, the access rights appropriate to the new role will be assigned to the user. This may result in loss of access rights.
Terminating access	Access rights are terminated and User IDs disabled when a person no longer works for NMDHB.
Auditing and monitoring	• Staff will be trained on security and privacy issues prior to receiving their login to the computer system. • All systems generate audit trails which identify the user ID and information accessed by it. • Adherence to this policy will be verified by examining the audit trails generated by the applications. • PERC conducts regular audits. • These audits can be performed at random, without notice, and cover individuals and whole departments for every information system. • Non-compliance or violation of this policy will result in appropriate action being taken in accordance with NMDHB disciplinary procedures. Compliance audits will be regularly undertaken for: • Accesses to information • Staff use of information • Internet and email use • Staff compliance with NMDHB Information Systems policies. Audit requests can be made to PERC in writing for: • Special request audits • High Profile patients. See Appendix 1 *Information System Audit*.
Inappropriate access	The co-ordinating Privacy Officer, and appropriate General Manager/Service Director will be advised if a breach of security is suspected as a result of the routine audit process. Further investigation and data gathering will be required to gain more information about the inappropriate access or security violation. This may involve Human Resource Department, Information Systems and the responsible Manager. Any alleged breach of policy will then be dealt with by the responsible Manager, with the assistance of Human Resources Department for further action, following current NMDHB policies.
Associated documents	NMDHB Information Systems *Access Agreement* (p.4) and *Access Deed*.
References	Health Information Privacy Code 1994 NMDHB policies: • Use of Information Technology • Disclosure of Client Information to the Police and other Government Agencies • Privacy: Disclosure of Client Information to Health Professionals & Principle Caregivers

APPENDIX 1 INFORMATION SYSTEM AUDIT

Audit Type	Audit Process	Expected Outcome	Action on Result
User access to and deactivation from NMDHB systems	User ID of terminated and transferring staff checked against state of account.	All terminated or transferring staff to have account deactivated or updated within 24 hrs of notification of cessation of employment or transfer.	CIO to be notified if standard not met.
High Profile Patient Audit	User ID matches to patient NHI for appropriateness of access.	All access to high profile patients, will be by those directly involved in care.	PERC to be notified of suspected inappropriate access. Manager of Service to be advised as appropriate.
Random Patient Audit	Audit of all activity logged against a NHI. Authorising Managers to assist in verification process.	All activity logged against NHI will be by staff involved in care.	PERC to be notified.
Random User Audit	Audit of all activity logged against a user ID.	User will be accessing information appropriate to their role within the organisation.	PERC to be notified.
User Compliance with IS policies and security awareness	Random “walkabout” audits of workplace practices.	For example: • Clinicians will be logging out of clinical applications • Passwords will not be openly displayed • Computers will be secured and shut down at end of the day.	Verbal feedback to staff. Letter to staff re compliance.
Data integrity Audit	Auditor completes normal activity within systems and tracks activity.	System tracks activity successfully.	Report any issues with audit tools to CIO.

ACCESS AGREEMENT

As a staff member or contractor, you are in the privileged position of having access to NMDHB's information, which might include other people's personal health information in the course of your work.

You are expected to act professionally and ensure confidentiality is maintained at all times. The information accessed shall only be that necessary for you to undertake your role.

This includes the health information of other staff members and your own family members who are a patient at Nelson Marlborough DHB. The Health Information Privacy Code 1994 applies to the hospital as a health agency and is intended to ensure the protection of individual privacy.

An outline of the Health information privacy code 1994 is included in your orientation pack or can be found on the NMDHB Intranet, please take the time to familiarise yourself with it. Ask your manager if you have any questions or you are welcome to contact Mike Cummins, Privacy Officer on extension 7997.

In addition to this policy, you will also be expected to comply with the following NMDHB policies:

- Use of Information Technology
- Disclosure of Client Information to the Police and other Government Agencies
- Privacy: Disclosure of Client Information to Health Professionals & Principle Caregivers

Nelson Marlborough DHB routinely audits staff access to information to ensure compliance. This may include an audit of information you have accessed over a period of time.

You shall not share your user ID and password with any other person.

Any breach of policy of either patient information or Nelson Marlborough DHB business information will be taken very seriously and could result in disciplinary action.

I understand the Confidentiality Requirement and will abide with it.

Signed _____ Date _____

Name Printed _____

Designation _____

Department _____