<Practice>
Cornerstone Policy
Section 2 Indicator 12
PRACTICE MANAGEMENT SYSTEM

Purpose

The policy outlines the systems and process that the practice use to ensure practice data and information safety and security.

Scope

The policy applies to all staff and any other personnel who have access at any time to Practice IT system and information that the Practice is privy to as part of their role as a medical home.

Policy

The Practice will ensure that all staff are familiar with the measures required by the practice for security of practice data and information systems.

All staff are required to read, understand and sign a confidentiality agreement that outlines their responsibilities for the practice data management and information security.

The practice orientation manual will document staff access to email and internet services that the Practice permits their staff to utilise. Staff will at all times be aware that the email system is inherently insecure.

All staff are advised and understand the computer lock out system and access this if they are going to be away from their computer for any length of time.

All staff are required to uphold the practice security policy and procedures. Staff must be aware of their obligations that they are storing, securing, transmitting and disposing of health information to at all times protect the privacy of patients.

The Practice has evidence of independent auditing of their electronic data systems and policies. The practice has an IT specialist external to the practice who has the expert knowledge and capability to provide a professional service.

Practice Manager

The practice has a nominated Practice Security Officer who may be the Practice Manager

The Practice Manager will provide each staff member with a login to access the Patient Management system. Each staff person will have an individual password of moderate security. All staff are responsible to change their password on a regular basis as per practice guidelines. Passwords are not shared with other staff members.

The Practice Manager is responsible for managing computer security. The Practice Manager will liaise with their IT vendor to ensure that the practice computers are protected with firewalls, antivirus and anti-spyware software.

The Practice Manager is responsible for all computer placements in a position that is not easily visible by the general public. Screen savers are set on a time frame that the Practice and their IT vendor have decided.

The Practice has documented evidence of independent auditing of their electronic data systems and policies.

The Practice Manager has a number of responsibilities with respect to the security of health information, including:

- Establishing and approving information security policies and procedures,
- Agreeing on specific methodologies and processes for information security,

e.g. risk assessment, security classification, etc.,

- Determining acceptable levels of security risks,
- Monitoring major information security threats and incidents,
- Approving major initiatives to enhance information security,
- Ensuring that formal audits are performed as necessary,
- Reviewing audit reports where security problems exist,
- Appointing the Practice Security Officer,
- Acting as the Authorised Signatory in respect to the issuance of digital certificates.

The policy defines how the practice meets the key elements of a good security policy.

Principles	Definition	Practice Implementation
Confidentiality	Assuring that a message is not readable by unauthorised parties whilst in transit.	Using password protected information
Integrity	Knowing that the message was not damaged or altered whilst in transit.	Using secure private networks
Authenticity	Assurance that the user is a trusted third party	The use of User ID/Password
Non-repudiation	Providing assurance that the sender cannot: claim that the message is counterfeit Deny that the message was sent	The use of private networks
Auditing	Recording of user connectivity and site access	Logging can be undertaken at sites and by the network provider
Accountability	Identification of clear responsibilities of organisations and individual users	Compliance with legislation and practice policy.

SECURITY

Security Incident Security Incident is an event and/ or condition that has the potential to impact on security or privacy and may result from either intentional or inadvertent action.

Security Violation A security violation is an event that may result in the disclosure of sensitive or otherwise classified information to unauthorised individuals, or results in unauthorised modification or destruction of system data, loss of computer system processing capability or loss or theft of any computer system resources.

Resources

- Health Regulation 1996- www.legislation.govt.nz
- Health Information Privacy Code 1994- www.privacy.org.nz
- Medical Council of New Zealand: www.mcnz.org.nz
- Maintenance and retention of patient records 2005
- Information and Consent 2002
- Confidentiality and Public Safety 2002
- Standards New Zealand AS/NZS ISO/IEC Information Technology / Security

- Standards New Zealand SNZ HB8169 2002 Health Network Code of Practice
- Standards New Zealand SNZ 8170 2005 Primary Healthcare Practice Management Systems

Title: Practice Management System	Section 2 Indicator12
Authorised: Carol Ennis 	Date: 17th November 2016
Review Date	Signature
Review Date	Signature