Security of Electronic Health Information Policy

1 SUMMARY

This security policy provides direction and process to address the following areas of concern:

- General security policy and standards
- Security organisation
- Personnel security and training
- Physical security
- Computer systems access control
- New Zealand Health Network
- Security in system life cycle management
- Computer integrity and incident reporting
- Malicious software
- Business continuity management
- Compliance

The evolving impacts on electronic health records including the safe storage and requirements for access necessitate that this policy be reviewed annually to ensure continued relevance and effectiveness.

The Privacy Policy should be read and followed in conjunction with this Policy

2 POLICY STATEMENT

2.1 Purpose

Electronic records are essential for managing and auditing patient information. Continuity of care requires that information is robust and available when needed so that practice teams can manage and track conditions. Effective electronic data is up to date, readily accessible, safely stored, and has an audit trail to meet Health Sector, Health and Disability Commission or other legal requirements.

This policy outlines the protocols that will be followed by staff working in this practice to protect continuity of electronic systems recording patient information. This policy also addresses the requirements of the Foundation Standard supporting the practice environment and safety.

2.2 Background

The Health Information Privacy Code 2020, Rule 5 – Storage and Security of Health Information, directs that the Practice has the role of responsible custodian of health and patient information and will therefore promote and help protect the privacy of personal information.

Most health-related information is collected in a situation of confidence and trust, is generally highly sensitive and may include particularly sensitive personal details which must be protected at all times.

2.3 Scope

This policy applies to all staff engaged in any activity carried out at this practice including those not directly employed by the practice e.g. Health Improvement Practitioners and Health Coaches etc.

2.4 Responsibilities

All staff are responsible for ensuring this policy is followed.

The Privacy Policy identifies who the Privacy Officer is for Doctors on Riccarton. Included in the responsibilities of the Privacy Officer is a requirement to ensure that requirements of the HIPC code including security of information are maintained.

2.5 Definitions & Abbreviations

HIPC	Health Information Privacy Code 1994
Health information:	is any information, such as medical history, disabilities, daily notes, classifications and screening results, dispensing record, discharge summaries, and test results, that can be associated to the patient the information relates to. Also includes any information of a personal nature such as contact details, next of kin etc.

2.6 Related Policies

- Privacy Policy
- Complaints Policy

3 POLICY DETAIL AND PROCEDURES

The principles of the Privacy Policy (confidentiality, collection, security, disclosure and transfer/destruction) are relevant when processing security requirements in line with this policy.

Security of Information

Health information will be stored securely with safeguards to prevent access by unauthorised people or its loss.

- Work areas are, as far as conveniently possible, will be kept clear of papers and removable storage media in order to reduce the possibility of unauthorised access, loss of, and damage to health or personal information during and outside normal working hours.
- Individual user accounts will be used for all access to programmes or files containing identifiable personal information or clinical records.
- There will be a password policy/enforcement of passwords to a required complexity.
- Time activated screen locking will be in place requiring staff to log on after 15 minutes of inactivity
- Filing cabinets, rooms and other areas used to store personal or health information will be locked when they are unattended
- Back-up of computer systems will be completed each working day with a data copy maintained off site at
- When required, the destruction of private information will be in a secure manner such as shredder, burning or by an approved document destruction contractor.
- No computer equipment that is sent or taken off-site for repair or sale, will contain sensitive or personal information unless appropriate contractual agreements are in place with third parties which include a confidentiality agreement.
- All application and operating system security updates will be installed when they become available on all devices. This includes devices at the work premise and on any devices used for remote access purposes.

Back up of Information

- Electronic health information is held on our cloud-based Practice Management System, Indici. Indici uses a Cloud Backup process of backing up data to multiple remote servers using continuous replication, i.e. Indici copies patient data to its servers as it changes. Should any one computer fail, including our Server, patient electronic health information can be accessed on any other computer.
- Back-up of our on-site server is provided daily by our PHO, Pegasus Health on remote servers. Patient data and documentation is only held on our server temporarily e.g. before uploading to Indici. Pegasus IT maintain their backup systems.
- Backup and retrieval testing of these backup systems is to be implemented by Indici and Pegasus Health IT
- Independent auditing of the Practice's electronic data systems and policies shall be implemented by Indici and Pegasus Health IT.

Virus Prevention

Precautions will be taken to both detect and prevent the introduction of malicious software.

- The practice will actively use firewalls, anti-virus software and other methods to provide protection against the introduction of malicious software such as computer virus, network worms or Trojan horses.
- All staff will be educated on the proper use of virus protection measures in order to maximise the effectiveness of such measures. This includes reporting any suspected virus-related issues to managers as soon as they are detected.
- Ensure software is up to date and all critical security patches are applied as soon as they are released.

Disclosure of Information

The Privacy Policy sets out practice policy in relation to the disclosure or transfer of personal or clinical information.

All staff will be required to sign a confidentiality statement in line with the Privacy Practice.

Transfer of Health Information

The electronic transfer of medical records will only be completed using a secure health network such as GP2GP. The transfer should be completed in no more than 10 working days and will require a written request and / or receipt confirming requirements.

No transfer of medical records will be undertaken using e-mail, social media or other unsecure methods.

4 REFERENCES

- Privacy Act 2020
- Health information Privacy Code 2020
- Health (Retention of Health Information) Regulations 1996
- HISO 10029:2015 Health Information Security Framework