Doctors on Riccarton
Helping you to better health

Doctors on Riccarton Information Technology Security of Electronic Health Information Policy

February 2017

Reviewed – August 2022

Version 4.1

Doctors on Riccarton

Helping you to better health

DOCUMENT INFORMATION

Title	Doctors on Riccarton
Author	Marina Chin (Practice Manager)
Version	4.1
Status	Final
Filename	DOR IT and Security of Electronic Health Information Policy

HISTORY

Version	Date	Description of changes
1.1	19/11/2011	
2.1	13/02/2017	
3.1	23/07/2019	Renamed document to include "Security of electronic health information Updated IT Service Providers and contact details
4.1	11/08/2022	Updated Table 1 Technical Support Providers

Doctors on Riccarton
Helping you to better health

Table of Contents

1 Introduction

1.1 Purpose

This document provides guidance to users of the computer systems of this Practice. Implementation of the policies herein will ensure adequate security for all information collected, processed, transmitted, stored, or disseminated as part of the Practice systems and major applications.

These security policies are consistent with New Zealand Government legislation including the:

- Health Information Privacy Code 1994
- Privacy Act 1993
- Health (Retention of Health Information) Regulations 1996

1.2 Contents

This security policy addresses the following areas of concern:

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

1.3 Document control

The Practice IT Security Officer is the Practice Manager who will periodically review this document and will be responsible for any modifications deemed necessary. Any feedback and suggested amendments in respect of this document should be provided in writing to the Practice Security Officer.

The Practice Manager will be responsible for approving security policy amendments.

2 General Security Policy and Standards

2.1 Objectives

To establish and maintain adequate and effective information security safeguards for users to ensure that the confidentiality, integrity and operational availability of Practice and patient information is not compromised.

Sensitive information must be safeguarded against unauthorised disclosure, modification, access, use, destruction, or delay in service.

Each user has a duty and responsibility to other Practice staff members to comply with the information protection policies and procedures detailed in this document.

2.2 Legal requirements

With specific reference to the Health Information Privacy Code 1994, Rule 5 – Storage and Security of Health Information, 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.

2.3 Security policy reviews

The standard and quality of the information security controls implemented at this Practice will be verified through periodic reviews to ensure compliance.

2.4 Sensitivity of 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.

There are two main types of sensitive information:

- health information collected and controlled in accordance with the Health Information Privacy Code 1994 [3] or with other relevant health-related legislation, and
- any other information provided on the Practice computer system that is sensitive for other reasons; such as commercial information, staff related information or any other information which may be considered sensitive.

See also section 4.2, “Information classification”.

3 Security Organisation

3.1 Policy statements

A management framework is required so that all those involved in the use or maintenance of the Practice computer systems can initiate, co-ordinate and control the implementation of information security effectively.

3.2 Practice Manager as Practice Security Officer

The Practice Manager has a number of responsibilities with respect to the role as the Practice Security Officer in the security of health information the co-ordination of security issues that affect the Practice, including:

- developing and reviewing security policies and plans,
- advising Practice staff on security matters,
- monitoring major information security threats and incidents,
- ensuring that formal audits are performed as necessary,
- ensure that all computer systems used in support of Practice functions are backed-up in a manner that mitigates both the risk of loss and costs of recovery,
- acting as the Authorised Signatory in respect to the issuance of digital certificates,
- ensuring that Practice security policies and standards meet all New Zealand Health Network requirements,
- liaising with the New Zealand Health Network Security Officer in respect to security matters that may affect other members of the New Zealand Health Network.

3.3 Staff Responsibilities

Any security system relies on the users of the system to follow the procedures necessary for upholding security policies. Practice employees are therefore expected to:

- uphold security procedures and policies,
- protect their user identification and passwords,
- inform the Practice Security Officer of any security issues, problems or concerns,
- assist the Practice Security Officer in resolving security issues,
- be especially aware of the vulnerabilities presented by remote access and be aware of their obligation to report intrusions, misuse or abuse to the Practice Security Officer,
- be aware of their obligations in the event that they are storing, securing, transmitting and disposing of health information to protect the privacy of patients.

With specific reference to The Health Information Privacy Code (1994), Rule 5 – Storage and Security of Health Information, users are included in the description as custodians of health and patient information and are required to promote and protect the privacy of personal information.

4 Personnel Security

4.1 Objectives

To ensure that employees are aware of information security threats and concerns, and are equipped to support the Practice information protection policies and procedures in the course of their daily work.

4.2 Non-disclosure information and security agreement

All employees involved in the collection, use and disclosure of health information must sign a confidentiality agreement.

Contract staff and outside organisations not already covered by an existing contract (containing the confidentiality agreement) are required to sign a confidentiality agreement prior to accessing Practice facilities.

4.3 Training

Computer users must receive appropriate training before using computer facilities and applications used by this Practice.

All employees of the Practice are to receive appropriate training and regular updates in Practice policies and procedures, including security requirements, legal responsibilities and business controls.

4.4 Disciplinary process

Doctors on Riccarton has the right to access any information stored on a Practice computer drive, including any emails that have been sent or received and internet logs.

Employees and contractors who may knowingly disregard a particular policy requirement, will be subject to serious disciplinary action including the possibility of dismissal.

5 Physical Security

5.1 Policy statements

All hardware, software, documentation, commercial information and health information held by the Practice is to be protected from disclosure, modification, or destruction. This is especially true if access may reveal information that can be used to eliminate, bypass, or otherwise render security safeguards ineffective or enable the disclosure of patient information.

Where identifiable health and other sensitive information is stored, processed, or transmitted, physical access to that information is to be restricted to authorised individuals.

5.2 General requirements

Areas in which information (both health and commercial) is stored are to be physically secure and access restricted to authorised personnel only. Access to documentation in respect to computer systems is also to be restricted to authorised personnel.

All persons, other than employees, who are granted access to Practice premises must be accompanied and their access restricted to those areas necessary for them to complete their tasks.

5.3 Clear desk and computer screen policy

Work areas are, as far as conveniently possible, to be kept clear of papers and removable storage media in order to reduce the possibility of unauthorised access, loss of, and damage to information during and outside normal working hours.

Similarly, screen savers are to be activated on all Practice computers.

Sensitive and critical Practice information, including computer media, is to be locked away when not required.

5.4 Equipment protection

All items of equipment are to be sited or protected to minimise the risks from environmental threats and hazards, and opportunities for unauthorised access.

5.5 Work performed outside secure sites

Security controls are to be in place to ensure authorised operations and that sensitive information is properly protected.

Computers used to process patient information from remote locations must meet Practice security requirements and have authorisation from the Practice Security Officer.

5.6 Storage of Information

Practice information stored on computer systems must be regularly backed-up so that it can be restored if or when necessary.

5.7 Destruction of information

All care and responsibility must be taken in the destruction of sensitive information.

5.8 Disposal of storage media

All sensitive information must be erased from computer storage media prior to disposal.

Similarly, no computer equipment that is sent or taken off-site for repair, should contain sensitive information.

Damaged storage devices such as hard disks may contain sensitive information that if disclosed could cause considerable embarrassment. Consideration should be given to not having a device repaired if information cannot be erased.

6 Computer Systems Access Control

6.1 Policy statement

Access to computer services and information should be controlled on the basis of Practice requirements.

6.2 Responsibilities

Access control responsibilities are as follows:

Practice Manager / Practice Security Officer

- Will determine and support the Practice access control strategy.
- Will ensure the satisfactory resolution of problems relating to the provision of user access when, significant changes are deemed necessary.
- Will ensure policies and standards address all Practice requirements.
- Will ensure that logon and system access procedures meet defined requirements.
- Will ensure that data and applications are safe in project development environments.
- Will assist users in their day-to-day use of Practice computer systems by performing basic account administration functions, including the unlocking of locked accounts, resetting passwords, providing user instruction.

6.3 Information system access control

Minimum requirements for information system access control are:

- valid individual user identifications and passwords for all computer access,
- new user accounts are to be initially configured so as to force a change of the password upon first logging on.

6.4 User logon procedures

Access to Practice computer facilities are to be via a secure logon process. The relative logon procedure will:

- not display system or application prompts until the logon process has been successfully completed,
- not provide help messages during logon procedures,
- validate the logon information only on completion of all input data,
- allow only three unsuccessful logon attempts before:
    - recording the unsuccessful attempt,
    - forcing a time delay before further logon attempts are allowed,
    - suspending a user account to prevent repeated invalid access attempts,
    - disconnecting and giving no assistance after a rejected attempt to logon,
- limit the time allowed for the logon procedure; if exceeded, the system should terminate the logon,
- display the following information on completion of a successful logon:
    - date and time of the previous successful logon,
    - details of any unsuccessful logon attempts since last successful logon.

This allows the user to check whether it was that he/she who was last logged on. If not, the incident should be reported and appropriate action taken.

6.5 Password standards

The following password standards are to be adhered to ensure compliance with the basic principles of logical security:

- the use of individual passwords is to be enforced to maintain accountability. Sharing of passwords is not permitted,
- users should be able to select and change their own password and be required to provide a confirmation to account for typing errors,
- a password is to have a minimum length of four characters,
- passwords are not to be easily guessed e.g. not car registrations, personal initials, dates of birth.
- maximum password lifetime for remote access is to be 90 days for normal user accounts and 60 days for system administrator accounts,
- users are to be forced to change temporary (initial) passwords at the first logon,
- passwords are not to be displayed while being entered,
- password files should be stored separately from the main application system data, and any access restricted to the system administrator,
- password files are to be stored in encrypted form, using a one-way encryption algorithm,
- default vendor user Ids and passwords are to be deleted or altered following installation of software.

6.6 Individual user account management

Inactive user accounts that are no longer required are to be disabled and identified as pending deletion.

The Practice Security Officer is to approve the continued availability of a particular inactive user account.

6.7 Electronic Mail

As electronic mail (e-mail) is a business resource, Practice personnel are to note that:

- personal use of e-mail is to be kept to a minimum,
- the e-mail system is inherently insecure and individuals other than the intended recipients may be able to read messages,
- nothing should be included in an e-mail message that would not be printed on Practice letterhead,
- the information contained in e-mail messages forms part of Practice business records,
- no sensitive information should be sent as part of, or attached to, an e-mail message unless the information is encrypted,
- e-mail attachments are a common source of malicious software and particular care is to be taken before opening any attachments, especially if the message is not from a trusted source,
- management reserves the right to monitor the content of e-mail messages.

All personnel should be aware of the security risks created by electronic mail including the vulnerability of messages and any legal considerations.

Using email

All personnel should only communicate with a patient via email if the patient has asked you to do so and is aware of the security risks associated with using email. You should document this conversation in the patient's notes before communicating with the patient via email. Where the email correspondence is important, you should copy and paste the email into the patient notes on your PMS.

Whenever you send an email to another health service provider or a patient you must:

- make sure that you type the email address correctly;
- make sure that your spelling and grammar is correct;
- use appropriate language; and
- make sure that the tone of your email is appropriate, bearing in mind the different ways that your message could be interpreted.

You must regularly monitor the emails that you receive and respond to any emails that require a reply as soon as possible.

When communicating with patients via email you must ensure that it does not breach the privacy obligations, is a secure mode of communication and the information is not sensitive.

You must advice patients on the limits placed on the use of email. For instance the patient should never seek urgent advice by email and sensitive information would never be communicated by email.

The patient should be advised of the risks associated with email communication and should consent to receiving that information after acknowledging and accepting the risks associated with security and privacy.

Receiving email from a patient should not be taken as consenting to receive personal information by email.

Prohibited email practices

In order to protect the reputation of Doctors on Riccarton and to ensure that staff use email appropriately, Doctors on Riccarton prohibits the following email practices:

- creating, sending or forwarding emails or email attachments that contain unsuitable material;
- creating, sending or forwarding defamatory, fraudulent or harassing messages (you should make sure that your emails do not contain any negative comments about patients or staff);
- creating, sending or forwarding emails that contain any material which is discriminatory on the basis of sex, age, race, ethical belief, marital status, religious belief, colour, ethnic or natural origin, disability, political opinion, employment status, family status or sexual orientation;
- creating, sending or forwarding emails that are not work-related, including email advertisements, electronic chain letters, and emails about pyramid selling schemes;
- creating, sending or forwarding excessively large emails; and
- using email unethically, such as sending emails from another person's email address or impersonating another email user.

6.8 External network connections and controls

Connections to other networks, including the World Wide Web, are to be protected through a firewall.

Firewalls must be properly configured so as to ensure the required level of security is achieved.

Default settings in network servers are to be changed so as to minimise the possibility of unauthorised access.

No software, or other material, is to be downloaded from the World Wide Web without the prior knowledge of the Practice Security Officer.

When using the internet all personnel should be aware that the internet contains:

- some material that is inaccurate; and
- some material that Doctors on Riccarton deems unsuitable for business use.

Files containing copyright material are not to be downloaded or shared using the company network.

All personnel must not create, access, download, store or forward any improper, objectionable or offensive material to any person outside of the practice or within the practice. This includes but is not limited to, any material that contains:

- racist or discriminatory material;
- sexually explicit material including pornography; or
- hacking material.

All personnel are not permitted to access some websites during work hours. These include but are not limited to :

- social networking sites such as Facebook or Twitter
- Trademe or Ebay
- Gambling sites

Doctors on Riccarton expects you to exercise good judgement when using the internet. This good judgement should extend to out of work hours in relation to placing comments or photo's on social networking sites. You are not permitted to use the practice email address, logo or trademark on the internet for non-work related activities.

Any actions that bring the practice into disrepute may be considered serious misconduct under the terms of your employment agreement resulting is disciplinary action, including the possibility of dismissal.

6.9 iPod, USB Sticks, CD, DVD and Text Messaging Usage

iPods may be used during breaks in the staff room, material is not to be downloaded using Doctors on Riccarton computer network

USB sticks, CD's and DVD's must not be used to transfer data to or from the Doctors on Riccarton network without consent from the Practice Manager

Use of text messaging is to be confined to tea and meal breaks.

7 Connected Health Information Services

7.1 Use of the Connected Health Information Services

Connected Health Information Services enable healthcare organisations to safely health information. The Ministry of Health is responsible to the sector for the delivery of these services. The Ministry is accountable for governance, management, some operational components, control and audit, and national service performance monitoring. This service and technology are continually evolving so information can be securely shared to enable integrated models of care.

Connected Health Information Services includes a number of services already in place such as:

- National Health Index (NHI)
- eSpatial Address Management (eSAM)
- GP2GP
- Access to other information services such as B4Schools and NIR data
- National Enrolment Service (NES), and
- New Zealand ePrescription Service (NZePS).

While this Practice has its own security requirements, it also has responsibilities in respect to the security of information in the Connected Health Information Services environment. These include:

- ensuring Practice security policies and plans are consistent with the requirements of the Connected Health Information Services agreement,
- ensuring all employees that use the service are aware of their security responsibilities,
- assisting the service in resolving any security issues where possible,
- revoking any digital certificates that were issued to employees who have resigned,.

7.2 Sensitivity of information

All information passing through the New Zealand Health Network will be regarded as highly sensitive and will be appropriately protected at all times.

7.3 Digital certificate management

Digital certificates are required for access to the Connected Health Information Services. The device on which any digital certificate is supplied is to be stored in a secure manner that permits access as and when required.

The Practice Security Officer is responsible for coordinating the issuance and renewal of any digital certificates issued to Practice employees.

The Practice Security Officer will formally request the Certification Authority to revoke a digital certificate in the event that:

- the digital certificate is stolen,
- a password becomes corrupted or known,
- a certificate holder leaves the employment of the Practice, or
- the certificate becomes redundant for any other reason

8 Security in System Life Cycle Management

8.1 Installation of software

The Practice Security Officer is to approve all software prior to it being installed.

8.2 Operational Software

Vendor supplied software used in operational systems is to be maintained at a level supported by the supplier.

Software patches that help to remove or reduce security weaknesses are always to be applied in a timely manner and with appropriate consideration for the seriousness of the risk an unpatched vulnerability poses.

8.3 Technical support and maintenance

Hardware and software maintenance activities are not to affect the integrity of existing safeguards or permit the introduction of security exposures (computer viruses, logic bombs, malicious code, etc.) into the Practice computer systems.

Automated dial-up diagnostic maintenance of sensitive applications by software vendors via remote communications is only to be undertaken under the direction of the Practice Security Officer.

9 Computer Integrity and Incident Reporting

9.1 Policy statements

All personnel are to comply with the software integrity procedures outlined in this document especially in respect to the following:

- security violations and software malfunctions reporting
- virus prevention and monitoring

9.2 Security incident

A 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.

All employees, and others likely to be involved, are to be made aware of the procedures for reporting incidents that might have an impact on the security of Practice assets and information.

9.3 Security violation

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

If a security violation occurs as a consequence of a user's access, that user and any like users are to be provided with guidance by the Practice Security Officer to ensure that the violation does not re-occur.

9.4 Reporting of security incidents or weaknesses

Any security-related incidents, violations or weaknesses, are to be reported to the Practice Security Officer at the earliest possible time but by no later than the following business day.

10 Malicious Software

Software and information processing facilities are vulnerable to the introduction of malicious software such as computer viruses, network worms and Trojan horses. It is therefore essential that precautions are taken to both detect and prevent the introduction of malicious software.

10.1 Virus prevention procedures

New viruses are being developed at regular and frequent intervals and could seriously undermine the integrity of the Practice systems unless they are prevented. Accordingly, all workstations are to have anti-virus software installed.

The Practice Security Officer is to ensure that virus signature files are updated on a regular (no less frequently than monthly) basis so as to ensure that any new viruses can be promptly identified and removed.

Each individual user must ensure that the anti-virus software is active on their workstation so that any potential viruses from external sources are identified and removed.

10.2 Virus education programmes

All users are to receive instruction as to how best prevent the introduction of computer viruses and other malicious software.

The Practice Security Officer is to therefore ensure that:

- users are aware that e-mail attachments may contain (often unknown) viruses or other malicious software.
- users immediately report attachments with suspicious file extensions (including .vbs, .shs, .pif and .exe) to the organisation's IT support help desk.
- users know to never launch e-mail attachments from their e-mail systems unless received from a trusted source, and then only after due care has been taken.

Disciplinary procedures are to be brought into play in the event that a user fails to follow designated malicious software procedures.

11 Business Continuity Management

Doctors on Riccarton has a business continuity management plan so as to minimise the effects of disruption caused by disasters and system failures (which may be the result of, for example, natural disasters, equipment failures, or deliberate actions) through a combination of preventative and recovery controls.

Plans are developed and implemented to ensure that Practice processes can be restored within a timely manner, and are to be maintained and practised so as to become an integral part of all other management processes.

IT failure can result from:

- Hardware failure – the hard drive in your server could develop a mechanical failure, develop bad sectors or have an electrical component fail.
- Software failure – software application errors, operating system crashes and computer viruses can all cause data to become damaged or corrupted.
- Natural disasters – power failure, and other events outside your control such as fire, flood, lighting strike etc.
- Human error.

To help avoid disaster Doctors on Riccarton:

- 3 systems of back-up. Off-site backup supplied by Pegasus IT, weekly hard drive backup, daily back up on an alternative computer.
- A server connected to a UPS (uninterruptible power source) –giving us time to shut down our server properly in the event of a power failure.
- Pegasus IT sends us a back-up log daily.
- Weekly hard drive back-ups are stored off site.
- The Practice Manager's computer is also backed up by Pegasus IT
- Use of the server is restricted.
- Antivirus and our operating system patches and service packs are updated.
- Our PHO have a robust firewall installed for access to the internet.
- Remote access has been set up by IT helpdesk at Pegasus, who make sure its security is as tight as it can be.

Table 1: Technical Support Providers

Support Type	**Provider**	**Phone**
Hardware	Pegasus IT	353 9990 ext 1
PMS (Indici)	Valentia Technologies	07 929 2090
Network System Support/Intranet	Pegasus IT Helpdesk	353 9990 ext 1
Off-Site Backup	Pegasus IT	353 9990 ext 1
Payroll software	Smartly Payroll	0800 10 10 38
Virus removal	Virus Busters NZ Ltd	359 5735 (021) 465 547

12 Compliance

12.1 Software Licence Compliance

All conditions of a vendor's software licence are to be strictly observed.

Users are responsible for ensuring that all licensing obligations are met and maintained.

12.2 Security Awareness

All users are to be kept aware of their general security responsibilities and be regularly updated. It is essential that users understand and adhere to procedures for managing, detecting and responding to security incidents.

The Practice Security Officer is to take responsibility for maintaining user security awareness.

12.3 Compliance with Security Policy

All security procedures are to be subject to periodic review so as to ensure compliance with Practice security policies and standards.

Similarly, information systems are to be checked for compliance with security implementation standards.

Audits of operational systems are to be planned and agreed so as to minimise risk of disruption to Practice processes.

12.4 Approved Non Compliance

Where a particular policy cannot be complied with for a substantive business reason, approval for a deviation from policy is to be obtained from the Practice Manager.

Requests for authorised non-compliance must be formally submitted with details of any risks associated with the deviation.

The Practice Manager will maintain a record of all approved non-compliance requests.

All approved non-compliance requests will be subject to six-monthly reassessments.