Basic Principles of Security *(New Zealand Health Network Security Policy for General Practitioners)*

The Do's:

Ensure that your computer equipment and premises are kept physically secure
The security of your equipment and premises is important, both to you and to the New Zealand Health Network. You are responsible for ensuring the physical protection of your computer systems that may be connected to the New Zealand Health Network.

Ensure passwords are selected carefully and kept confidential at all times
Each user is expected to be accountable for any actions that take place under that user's user-Id and password. We strongly recommend passwords of at least 8 characters that contain a combination of capital letters, lower case letters and numbers.

Use different passwords for different log-ins
Using the same password to log into all security systems presents a risk to your online security. If an online attacker obtains the single password, they have access to all security systems you utilise. A different password for each security system to use reduces this risk and increases your levels of protection.

Ensure that anti-virus software has been installed and activated on each computer, and is regularly updated
Computer viruses will be disruptive if not destructive; to both your practice systems and to the New Zealand Health Network. Ensure that preventative measures are in place. Computer games should not be downloaded from the Internet.

Ensure that all users are aware of their security related responsibilities - security is dependent on people more than it is on technology
By far the greatest source of security related problems are attributable to authorized users of computer systems. Adequate and proper training in office procedures and use of computer systems is essential.

Report any security-related incidents to Pegasus
It is important that any incidents affecting security are reported to Pegasus to ensure the Pegasus, CDHB or New Zealand Health Network is protected.

The Don'ts:

Share your passwords or write your passwords down and leave them around your desk or computer/laptop
Treat your password as though it was used for your personal online banking. If you know someone else has become aware of your password, change it immediately. If you allow a colleague to use your credentials and in-appropriate use occurs it is your responsibility.

Introduce new software to your computer without first running an anti-virus program
No new software should be seen as coming from a trusted source; prevention is the key to better security. Pay particular attention to any games that a user may attempt to download from the Internet.

Use your administrative systems password for web access or e-mail purposes
In that way the inadvertent disclosure of one password will not compromise the security of other systems.

Store non-essential sensitive information on local systems
Sensitive information stored on local systems should be limited to that which is necessary for the well-being of individual patients.

Allow Pegasus, CDHB or New Zealand Health Network access to other than the areas required by the user
"Browsing" other information throughout the network is not to be permitted. It is best to allow access to information on a "need to know" basis only.