



Section D: Information management

Indicator D.10.2

Electronic health records are used in the practice.

Electronic notes are now essential for the management and auditing of patient information – it is the only way to provide accurate accessible data and an audit trail of activity for the Health and Disability Commission or legal requirements.

The checklist is to provide guidance only and does not constitute a comprehensive or exhaustive tool on the subject matter or method of verifying compliance.

The text is directed at health professionals who hold a qualification in medicine or healthcare and who are trained and are skilled in regard to information technology. Persons implementing the policy must exercise their own independent skill and judgement or seek appropriate advice as to reliance upon the guide, which may require modification in light of the risk profile of their particular practice or circumstances.

The practice must act with due diligence to determine whether their policy meets their needs and that the content aligns with all legal, ethical and moral obligations.

Information Technology		
IT CATEGORY	TASKS	INTERPRETATION
Practice computer security coordinator D.10.2-5 D.11.2-3 D.11.4-1 D.11.4-2	Practice IT security coordinator appointed Practice IT security coordinator’s role description written Date for review of security coordinator’s role	Need not be separate policy - may be part of an individual’s job description Annually as part of D.11.2-3, D.11.4-1 D.11.4-2
Practice IT security policies and procedures A.1.3-4 D.10.2-5	Person(s) (e.g. IT security coordinator) appointed to document (and revise) security policies and procedures (can be part of practice manual) IT security policies and procedures documented IT security policies and procedures documentation last reviewed... IT security audited regularly – 6 monthly.	Reminder to include portable hardware security - portable flash-drive keys and laptops. Commercial desirability of information and risk of breach of Health Information Privacy Code 1994 Password protected / backup of laptop data. Passwords checked Virus protection up to date Backups verified Staff can describe the security measures, e.g. passwords, screen savers Security coordinator shall ensure that all instructions and procedures in the security policy are being followed, e.g. change of passwords

RNZCGP CORNERSTONE General Practice Accreditation Programme 2009

	<p>Staff trained in IT security policies and procedures</p> <p>Copy of Health Intranet policy held in practice</p> <p>Electronic mail policy – if used</p>	<p>Taking reasonable steps before a computer interface is established with a system to ensure the arrangement does not increase the risk of unauthorized access.</p>
<p>Access control D.10.2-5</p>	<p>Staff policy developed on levels of electronic access to data and systems</p> <p>Staff have created personal passwords to access appropriate level Passwords are kept secure</p> <p>Change passwords periodically</p> <p>Restriction on physical access to the server – designated personnel only</p>	<p>Restricting access to documentation around installation and computer systems to authorized personnel NZS 8153:2002.</p> <p>Passwords are not easily 'guessed' (e.g. not names of pets, personal initials, preferable at least 4 digits long containing a combination of letters and digits)</p> <p>Only authorized personnel have physical access to the server I.e. can add, remove or change any server hardware.</p>
<p>Disaster recovery plan D.10.2-6</p>	<p>Disaster recovery plan developed – business continuity management Date disaster recovery plan last tested Date disaster recovery plan last updated</p> <p>Irreplaceable data is saved on the server not on hard drives of individual PCs on the network</p>	<p>In a recovery plan: How to continue to make appointments Issue patients with invoices and receipts Enable doctors to provide adequate clinical care while not having access to electronic medical records Who to phone for technical support How to restore data using the backup medium Restoration to normal working conditions if possible Additional roles that staff may be required to undertake while 'disaster' active. Including backup of laptop data Data is backed up regularly</p>
<p>Consulting room and 'front desk' security A.1.4-1 D.10.2-6</p>	<p>Practice aware of need to maintain appropriate confidentiality of information on computer screens</p> <p>Screensavers or other automated privacy protection device enabled – timely activation</p>	<p>Passwords not to be shared Screensavers in use Positioning terminals and personal computers so that they cannot be seen by unauthorized personnel</p> <p>Password protected screensaver in active use Activates in a timely manner Or other automated device in use</p>
	<p>Back-ups of data done daily</p>	<p>Essential data should be backed up daily At any time there should be at least two complete backups stored on the practice (both less than four days old) plus two complete backups stored at the other secure location (both less than 15 days old).</p>

RNZCGP CORNERSTONE General Practice Accreditation Programme 2009

<p>Back-ups D.10.2-6</p>	<p>Back-ups of data stored offsite - preferably in a fireproof safe</p> <p>Back-up procedure last tested - (use of 'verify function')</p> <p>Staff replace the tapes on a regular basis - if tapes in use</p>	<p><i>Gold standard - Fireproof safes must be certified as appropriate for magnetic media - able to withstand the temperature that could destroy backup disks and tapes.</i></p> <p>Back-up tapes should be stored with a high level of protection from physical and environmental risk.</p> <p>Run verification function to ensure data is available from the tape or check data e.g. date of modification, file size</p>
<p>Viruses</p>	<p>Anti-viral software is installed and functioning on all computers</p> <p>Automatic updating of viral definitions is enabled on all computers.</p> <p>Staff are aware of the practice policy on intranet and email use including security measures</p>	<p>Viruses interfere with the computer programme.</p> <p>The Intranet will be as secure as its weakest link - usually staff managing and using 'the net'.</p> <p>Examples: What constitutes reasonable private use (use that does not interfere with work efficiency)</p> <p>Websites that are not appropriate to view (pornography and other offensive sites)</p> <p>Inappropriate personal use of email - contains offensive or sexually harassing content</p> <p>Protection against SPAM</p> <p>Protection against viruses</p> <p>Protection against hackers</p> <p>Protection against the theft of information</p> <p>Protection against spyware</p> <p>Backing up email and internet favourites or bookmarks</p>
<p>Firewalls</p>	<p>Hardware and/or software firewalls installed (regardless of Broadband or dial-up access)</p>	<p>A firewall is an electronic mechanism that blocks unauthorized access into a computer system.</p>
<p>Network maintenance D.10.2-5 E.12.3</p>	<p>Computer hardware and software maintained in optimal condition - the practice has a budget for hardware and software maintenance and upgrade.</p> <p>Uninterruptible Power Supply installed (to at least the server) already covered above</p>	<p>The age and physical capacity of practice hardware should be recorded in an asset register and reviewed regularly as part a hardware cycle to ensure the hardware and software is appropriate for the work.</p> <p>A UPS is a device that contains batteries to enable computers to shut down smoothly when the main power supply suddenly cuts out. This is important so that data that is being processed while the blackout occurs is not lost. UPS also help with power surges.</p>

References:

- Health Information Privacy Code 1994
- Information Technology Risk Management resource for New Zealand General Practice Feb 2005 (RNZCGP in draft)
- New Zealand Health Network Code of Practice 2002
- New Zealand Health Records 2002
- Privacy Act 1993
- Standards New Zealand Health Records NZS 8153:2002

Additional Helpful Resource:

www.gpcg.org.au May 2007 Security Guidelines