Good IT Practices: Recommendations for good IT management for general practices

General practices are increasingly dependent on their IT systems for managing their patients and their business. Up to date and effective IT systems are an essential part of protecting electronic patient information against the risks of data loss or unauthorised access.

As other technology solutions move forward it is also important to ensure that the IT platforms that you operate are able to support new IT systems aimed at helping the practice to improve performance and patient outcomes. The following are some recommendations for good practice IT management.

1. Effective backups

- Effective and properly managed backups are the most important defence against loss of data that could result from many different issues, including hardware failure, computer virus infection or physical events such as fire
- Backup schedules should be performed at a minimum of daily (differential – where all changes since the previous backup are captured), weekly (full backup – where all data is captured) and end of month (full backup)
- These should be stored offsite in a secure location on a daily basis
- Backups should be validated to check that they have been successfully completed and tested at least once a month to ensure that they are valid and recoverable

2. Antivirus, security updates and firewalls

- A subscription based reputable anti-virus solution should be deployed (e.g. Symantec, ESET, McAfee) and each workstation should have a full scan scheduled on a weekly basis
- Updates (such as Windows Updates) should be regularly applied to ensure that systems are fully patched against vulnerabilities
- Use firewalls to protect your systems from unauthorised network traffic
- Use an email security system such as MailMarshal

3. Use of up to date IT hardware and operating systems

- All IT equipment should be kept current. Old equipment has a higher likelihood of failure.
- As a guide, any equipment older than five years should be considered for replacement
- IT operating systems (such as Windows Server or Windows for the PC) should be kept within current supported versions
- Microsoft XP support ended in April 2014 and Microsoft Server 2003 support will end in July 2015. Desktop and server computers using these operating systems will become vulnerable as no new security updates will be provided. Practices should be working with their IT provider on a plan for upgrading any computers using these operating systems.

4. Practice management systems – database management

- Appropriate database management should be undertaken for the practice management system (e.g. Medtech32) and the required maintenance schedule followed as prescribed by the relevant software vendor

5. Security, awareness and vigilance

- System access should be protected by robust passwords which are kept secure and regularly changed (at least every 90 days). Passwords should be at least 8 characters long (the longer, the better), contain a mixture of upper and lower case characters, numbers and symbols and should avoid words that could easily be associated with the user.
- Care should be taken with any suspicious emails, and particularly before opening any attachments included with suspicious emails. Suspect emails should be deleted.
- Practices should have policies in place to manage risks associated with copies of sensitive data held on portable media and devices (such as USB data sticks, mobile phones, tablets and laptops). At a minimum, access should be protected by passwords or PIN numbers and where possible, avoid copying sensitive data to these devices.

6. Trusted and reputable IT service providers

- Engage a trusted and reputable IT supplier, and ensure that your IT provider has the necessary experience
- All support agreements with IT providers should be in writing. The contract should be clear on what services they will provide and on what terms, the service levels that they are committing to and any exclusions that may be in the "fine print". Practices should be able to confirm that their IT provider actually complies with all terms of the contract.
- Any vendor delivering IT services for primary health that includes maintenance of Medtech32 should be MedTech or equivalent certified within the last two years