

## Computer Security for Practices

Securing your computers protects them from physical damage, data loss and unauthorised or inappropriate access. There are many measures practices can take that are cheap, quick and easy to implement and can make a big difference to the security of their systems:

### Physical security

- Have a dedicated server and position it away from patient traffic, preferably in a locked room.
- Buy a floppy drive lock and locking wires for the server.
- Position screens so that they are not visible and/or accessible to the patients.
- Position faxes and printers so that patients cannot see or access the output.
- Tapes/disks, faxes and computer printouts should be positioned or stored out of sight when not in use.
- Have physical security on the building – locks, alarms etc.
- Laptop and palmtop computers should hold the minimum amount of data necessary and should be stored in a secure physical location when not in use (eg. safe or locked room). While in use, laptop and palmtop computers should not be left unattended at any time.
- Have an uninterruptible power supply (UPS) on the server to protect against power supply problems that could cause data loss or corruption.
- Have surge protectors or mini-UPS on the workstations and hub/switch.
- Tapes/disks and computer equipment should be positioned away from environmental hazards such as extreme heat or cold, direct sunlight, high or low humidity and magnetic fields.
- Avoid smoking, eating or drinking close to computer equipment or tapes/disks.

### Software security

- Blank passwords, particularly administrator passwords and/or easy to guess user passwords mean easy access to confidential files if the computer is stolen or there is no firewall protection.
- Individual accounts are more secure than 'group' user accounts (eg. 'doctor' or 'reception') particularly when the password is not changed if a member leaves.
- Use boot passwords on laptops so that the system can't be used or the BIOS settings changed without using a password.
- Sharing out only the individual folders that are required by others on the internal network (ie. not the whole of C: drive).
- Windows files and folders can be secured by assigning permissions to groups of users. A lack of file/share level security can mean unauthorised or inappropriate access by staff or patients.
- Lock the computer when a doctor leaves the room. Although individual programs often have their own locking mechanism, it is best to lock the computer to prevent unauthorised access to all programs – on Windows 200x and XP this is Ctrl+Alt+Del then K.
- Have up-to-date virus protection and a procedure for ensuring it is kept updated. Many antivirus software packages now come with an update and alert feature to allow new updates to be downloaded from the Internet as soon as they are published.

- Use a firewall and make sure it is properly configured. A firewall isolates your internal system from the Internet and checks traffic to determine whether it should be allowed to pass through or should be blocked.
  - Firewalls can be hardware or software based. If you are planning a broadband connection to the Internet, choose a router that has port forwarding or network translation features and have this installed in a two network card (double-NIC) configuration so the internal practice network is isolated from the external network (router/Internet). Gateway configurations are insecure.
  - A firewall purchased but without proper configuration it is like a patient fulfilling a prescription but not taking the drugs!
  - If you are unsure if your system is secure, try ShieldsUp! from [www.grc.com](http://www.grc.com). This is a free, quick and accurate check of your practice's security.
- Ensure your backups are being done and checked, that backups are stored off-site and backup media is stored in secure locations.
- When disposing of outdated computer equipment or backup media, disks should be permanently erased or damaged to prevent re-use before disposal. Data on paper copies should be shredded.

### **Connectivity security**

- Gateway configurations where the broadband router is plugged into the internal hub/switch are not secure installations.
- Incorrectly configured routers and firewalls pose a security threat.
- Have non-routable IP addresses on local network (these are in the ranges 10.0.0.x or 192.168.x.x).
- Use secure methods of transmitting data.

### **User awareness of need for security**

- Doctors and staff need to be made aware of the dangers of poor security – medico-legal issues, accreditation issues, patient confidentiality, privacy etc.
- Doctors and staff may mistakenly believe everything has been correctly installed and configured by IT experts.
- Reduce inappropriate use of e-mail/Internet/installation of programs by having clearly defined 'acceptable use' policies that are conveyed to all staff.
- Staff members, temporary staff and contractors that require access to the Practice's systems should be required to sign confidentiality / non-disclosure agreements before commencing work.
- Train doctors and staff in security procedures and safe practices and ensure new staff are briefed - staff turnover can result in history/knowledge gaps.
- Use a policy and procedure manual that covers computer operations and security.
- Implement secure methods of transmitting data.
- Have 3-year on-site warranties for equipment with trusted local suppliers.

### **Summary**

'Reasonable' security at a 'reasonable' price should be within the grasp of any GP practice that has computers - buy wisely, configure correctly and implement security policies.