Criterion C6.4 – Information security

Indicators

C6.4►A Our practice has a team member who has primary responsibility for the electronic systems and computer security.

C6.4►B Our practice does not store or temporarily leave the personal health information of patients where members of the public could see or access that information.

C6.4►C Our practice's clinical software is accessible only via unique individual passwords that give access to information according to the person's level of authorisation.

C6.4►D Our practice has a business continuity and information recovery plan.

C6.4►E Our practice has appropriate procedures for the storage, retention, and destruction of records.

C6.4►F Our practice has a policy about the use of email.

C6.4►G Our practice has a policy about the use of social media.

Why this is important

Maintaining the privacy and security of health information held by a practice is a legal obligation. This includes maintaining the security of computers and other devices.

As practices are increasingly using electronic communication to communicate with patients and other health professionals, an email policy and a social media policy will help to protect the security of patient information and the reputation of the practice.

Meeting this Criterion

The current edition of the RACGP's *Computer and information security standards* (CISS) contains:

- information about security issues
- recommendations about how to protect against potential loss of sensitive data
- templates you can use to create policies and procedures relating to information security and the use of computers.

You could refer to CISS (available at www.racgp.org.au/your-practice/standards/computer-and-information-security-standards) to help satisfy the requirements of this Criterion.

Designated practice team member

Your practice must have a designated practice team member who has the primary responsibility for computer security. These responsibilities must include:

- knowing who and when to call for expert advice
- giving relevant practice team members the contact details of any external expert the practice has used

- educating the practice team about data security and the need to follow security protocols and policies
- monitoring whether team members are following security protocols and policies.

Keeping health information concealed

Computer screens must be positioned so that only appropriate members of the practice team can see confidential information. Automated privacy protection tools (such as screensavers) must be used to prevent unauthorised access to computers when they are left unattended (eg when a practitioner leaves the consultation room to collect equipment, medication or information).

Mobile phones, tablets, laptops and other portable devices and the information stored or accessed on them need to be as secure as your practice's desktop computers and network. This is particularly important because they are potentially more accessible to people outside the practice.

Restricting access to clinical software

Practice team members only require access to the information they need to undertake their roles. If you have given different members of the practice team different levels of access to patient health information:

- document who has access to different levels of patient heath information data
- make sure that practice team members understand why they must keep their passwords private.

Business continuity and information recovery

If your practice uses computers to store patient health information, you must have a business continuity plan to protect information in the event of an adverse incident, such as a system crash or power failure.

The business continuity and information recovery plan needs to include:

- the processes by which all critical information relating to the practice's operations (such as appointments, billing and patient health information) will be frequently backed up
- a schedule of regular tests so that backups are being correctly created and can be accessed and read as expected
- details of the secure offsite location where the backup information is stored
- standard letters of agreement that external IT providers sign to indicate their commitment to comply with the requirements of the CISS.

Replacing IT equipment

When IT equipment needs to be replaced or upgraded, refer to the current edition of the RACGP's *Effective solutions for e-waste in your practice* to ensure that you do not inadvertently lose or transfer key information. Just deleting records does not actually remove the data from a computer system, which means that people may still be able to recover files that have been deleted but not removed.

Other equipment, such as photocopiers and fax machines, may have hard drives that contain confidential information that must be properly removed before you dispose of them.

Destroying information

If you are considering destroying clinical records for patients who are no longer patients of the practice, have not been seen for many years, or who have outdated results in their records, consult with your medical defence organisation so that you understand your legal requirements and manage the risks.

If your practice has a policy to destroy these records, you must also have a system that provides timely identification of information that is no longer relevant.

You also need to have processes for the disposal of hard drives and other storage media.

Email and social media policies

If your practice uses email and social media, you must have policies for their use. The practice team must be familiar with the policies, comply with them, and understand the risks associated with using email and social media. The policies could also be made available to patients.

A policy for use of email in the practice may include information about:

- maintaining passwords and keeping them secure
- verifying and updating email addresses
- informing patients of possible risks to their privacy if standard unencrypted email is used
- obtaining patient consent to communicate with them via email.

For further information, please refer to the RACGP's *Using email in general practice – Guiding principles* at www.racgp.org.au/your-practice/ehealth/protecting-information/email

If your practice does not use email, have a policy that states this.

Practitioners registered with AHPRA are required to comply with AHPRA's social media policy.

The RACGP's *Guide for the use of social media in general practice* contains guidance for the safe and professional use of social media in a general practice. It also contains a template for a social media policy (which complies with AHPRA's social media policy) that you can adapt to suit your practice. It is available at www.racgp.org.au/your-practice/ehealth/social-media/guide

Meeting each Indicator

C6.4►A Our practice has a team member who has primary responsibility for the electronic systems and computer security.

You must:

- have at least one team member who has primary responsibility for the electronic systems and computer security.

You could:

- maintain a policy addressing the management of patient health information
- create a position description outlining the roles and responsibilities relating to computer security.

C6.4►B Our practice does not store or temporarily leave the personal health information of patients where members of the public could see or access that information.

You must:

- maintain a privacy policy.

You could:

- maintain a policy addressing the management of patient health information
- have a physical layout that means that members of the public cannot view patient health information
- use password-protected screensavers

- use a shredder and/or have a secure document-shredding agreement with a reputable provider
- wipe all information off hard drives and photocopiers before disposing of them.

C6.4►C Our practice's clinical software is accessible only via unique individual passwords that give access to information according to the person's level of authorisation.

You must:

- maintain the security of the clinical software passwords of each individual practice team member
- maintain a privacy policy.

You could:

- maintain an information technology policy
- give only appropriate access to each role, based on position descriptions
- ensure that staff members are trained to log out or lock computers and other devices after each use
- maintain a register of who borrows or takes a laptop or mobile phone
- maintain secure passwords for portable devices
- install current antivirus software on all devices.

C6.4►D Our practice has a business continuity and information recovery plan.

You must:

- operate a server backup log
- maintain up-to-date antivirus protection and hardware/software firewalls
- maintain and test a business continuity plan for information recovery
- maintain a privacy policy.

You could:

- maintain a policy for the management of patient health information
- undertake regular privacy training
- store backups offsite in a secure location.

C6.4►E Our practice has appropriate procedures for the storage, retention, and destruction of records.

You must:

- maintain and test a business continuity plan for information recovery
- maintain a privacy policy.

You could:

- maintain a policy for the management of patient health information
- maintain an information technology policy
- undertake regular privacy training.

C6.4►F Our practice has a policy about the use of email.

You must:

- maintain an email policy.

You could:

- put your email policy on your website
- have an automated response to patient emails that advises them of when they are likely to receive a response.

C6.4►G Our practice has a policy about the use of social media.

You must:

- maintain a social media policy.

You could:

- put your social media policy on your website.