Step 7 – Employ Safeguards

A practice must implement reasonable security safeguards to protect personal information against loss, theft or other unauthorized access, use or disclosure. Safeguards refer to administrative, physical and technical measures, and may include a combination of policies, practices and software that protect personal information. The sensitivity of the personal information informs what types of safeguards are appropriate in the circumstances, irrespective of the form in which a medical record is stored (paper, electronic, digital, or otherwise). For more information, see Guidelines for Protecting Medical Records Outside the Practice.

Medical records must be handled in a secure manner from the time the records are created to the time they are disposed of, regardless of the format in which the information is stored.

The following are best practices in safeguarding medical records and other personal information stored by the practice. Note that a combination of measures may be required during the transition from paper-based medical records to EMRs where both methods of record-keeping may be used in parallel.

In order to protect medical records, it is recommended that staff:

- wear building passes/photo ID if issued
- verify that persons who don't look familiar have a legitimate reason to be there
- know how to respond if suspicious behaviors are noticed
- not disclose confidential information about how the practice's security systems operate
- sign confidentiality agreements that specify obligations and expectations including consequences for inappropriately collecting, using or disclosing personal information

Paper records should be:

- retrieved promptly from fax machines or photocopiers
- clearly labelled
- placed in a location that prevents members of the public from viewing the records (e.g., avoid leaving medical records at the reception desk where other patients can see them)
- returned to the filing location as soon as possible after use
- stored:
    - on-site wherever possible
    - securely within the practice (e.g., in locked cabinets)

- in a location where members of the public cannot access the contents (e.g., in a locked, separate room)

- tracked if being transferred by confirming that the records have arrived at their specified destination
- kept secure at all times if taken off-site

In order to protect personal information stored in EMRs, staff should:

- when using any system or application, log out of computer systems or applications when not in use or unattended
- keep workstations positioned away from public view and access
- memorize or use a secure password manager instead of writing down passwords
- not share an assigned user ID and password with others

The privacy officer should also do the following to protect personal information stored in EMRs:

- Create a unique user ID and strong password for every authorized user.
- Grant role-based access to staff working in the practice on an individual basis based on a "need to know" and "least privilege" principles.
- Revoke user IDs and passwords as soon as authorized users resign or are dismissed.
- Install strong, up-to-date, industry-standard encryption.
- Implement password changes forced at regular intervals.
- Install firewall software and regularly update internet-based computer systems.
- Create audit trails to track when a patient record is accessed and by whom, including date and time.
- Verify that data backup methods and disaster recovery plans are in place and are periodically reviewed and tested.
- Activate password protected screensavers or auto log out for computers after a period of inactivity to avoid unauthorized viewing.
- Consider installing a privacy screen filter to prevent viewing of the screen from an angle.

For more information, see Guidelines for Electronic Medical Records and Role-Based Access.