

For the purpose of increasing your CPD points

ETHICS ARTICLE

Retention of medical records

Medical Protection Society

*Reprinted with permission from the Medical Protection Society: www.medicalprotection.org
Correct as of September 2011*

All healthcare professionals should appreciate the value of keeping accurate, detailed medical records for each patient. However, many doctors are unaware of how to manage medical records and do not know when it is permissible to dispose of them. This factsheet outlines the principles for retaining medical records.

Retention of medical records

It is good practice for every healthcare organisation to have a records management policy in place.

Good records management is essential for the continuity of care of your patients, and can reduce the risk of adverse incidents through misplaced or untraceable records. Problems with medical records - lack of accessibility, poor quality information, misinformation, poorly organised notes, misfiling, and many others - are known to lie at the root of a high proportion of adverse incidents.

It is good practice for every healthcare organisation to have a records management policy in place. An individual should be nominated as the person responsible for reviewing the policy on a regular basis and ensuring it is up-to-date with legislative requirements. Familiarise yourself with the following two record management standards:

- ISO standard ISO/IEC 27002: 2005 - which contains information on security issues such as staff responsibilities and training, premises, business continuity, protocols and procedures, email and internet usage policies and remote access. This standard has been approved for use in South Africa as SANS 27002:2008.
- ISO 27799: 2008 - Health Informatics: Information Security Management in Health - which contains all the relevant guidance in ISO/IEC 27002 as it relates to the healthcare sector.

Retention

The HPCSA offers the following guidance on the retention of medical records:

- Records should be kept for at least six years after they become dormant.
- The records of minors should be kept until their 21st birthday.
- The records of patients who are mentally impaired should be kept until the patient's death.
- Records pertaining to illness or accident arising from a person's occupation should be kept for 20 years after treatment has ended.
- Records kept in provincial hospitals and clinics should only be destroyed with the authorisation of the deputy director-general concerned.

- Retention periods should be extended if there are reasons for doing so, such as when a patient has been exposed to conditions that might manifest in a slow-developing disease, such as asbestosis. In these circumstances, the HPCSA recommends keeping the records for at least 25 years.
- The cost and space implications of keeping records indefinitely must be balanced against the possibility that records will be found useful in the defence of litigation or for academic or research purposes.
- Statutory obligations to keep certain types of records for specific periods must be complied with (see HPCSA, *Guidelines on the Keeping of Patient Records* (2008), paragraph 9.)

Disposal of medical records

Be wary of selling or donating second-hand computers – 'deleted' information can often still be recovered from a computer's hard drive.

An efficient records management system should include arrangements for archiving or destroying dormant records in order to make space available for new records, particularly in the case of paper records. Records held electronically are covered by the Electronic Communications and Transactions Act, which specifies that personal information must be deleted or destroyed when it becomes obsolete.

A policy for disposal of records should include clear guidelines on record retention and procedures for identifying records due for disposal. The records should be examined first to ensure that they are suitable for disposal and an authority to dispose should be signed by a designated member of staff.

The records must be stored or destroyed in a safe, secure manner. If records are to be destroyed, paper records should be shredded or incinerated. CDs, DVDs, hard disks and other forms of electronic storage should be overwritten with random data or physically destroyed.

Records pertaining to illness or accident arising from a person's occupation should be kept for 20 years after treatment has ended

Be wary of selling or donating second-hand computers – ‘deleted’ information can often still be recovered from a computer’s hard drive.

If you use an outside contractor to dispose of patient-identifiable information, it is crucial that you have a confidentiality agreement in place and that the contractor provides you with certification that the files have been destroyed.

You should keep a register of all healthcare records that have been destroyed or otherwise disposed of. The register should include the reference number (if any), the patient’s name, address and date of birth, the start and end dates of the record’s contents, the date of disposal and the name and signature of the person carrying out or arranging for the disposal.

Protecting paper records

If you keep a large quantity of paper records, you must ensure there are systems in place to protect them.

Paper records can be easily damaged by moisture, water, fire and insects. As paper records are irreplaceable, it’s a good idea to carry out a risk assessment to identify ways in which to safeguard them. If you keep a large quantity of paper records, you must ensure there are systems in place to protect them in case of fire, flood or other circumstances that could damage the records.

You must ensure you install smoke and fire alarms to allow you to act quickly in the event of a fire breaking out. Water sprinkler systems can damage electronic equipment so install chemical fire extinguishers to protect your paperwork.

Avoid storing archives of paper records in a basement as they are prone to flooding - instead, store records above floor level and ideally on a high shelf.

It is also important to conduct regular inspections of your premises and have control measures carried out by experts to keep damaging insects and rodents at bay.



Protecting electronic records

Electronic records should be regularly backed up and the back-up disk should be kept at a secure off-site location.

Electronic records should be regularly backed up and the back-up disk should be kept at a secure off-site location. Do not be tempted to keep your computer back-up drive in a fire-proof safe - if a fire breaks out, it can melt. Instead, use secure off-site storage wherever possible. If you have sprinklers in areas that house computers which contain electronic copies of medical records, put waterproof covers on the computers before going home at night.

CPD QUESTIONNAIRE

SURNAME

INITIALS

YOUR HPCSA REGISTRATION NO. **MP**

Address:

Telephone:

Fax:

E-mail:

Questions

True or false:

- | | | | |
|---|---|-------------------------|-------------------------|
| 1 | It is law for every healthcare organisation to have a records management policy | ☐ T | ☐ F |
| 2 | The back-up disk of electronic records should be kept at a secure on-site location | ☐ T | ☐ F |
| 3 | The records of minors should be kept until their 21st birthday | ☐ T | ☐ F |
| 4 | Water sprinkler systems must be installed to protect paperwork from fire | ☐ T | ☐ F |
| 5 | Electronic records are covered by the Electronic Communications and Transactions Act | ☐ T | ☐ F |
| 6 | Records of illness or accident arising from a person's occupation should be kept for 20 years after treatment | ☐ T | ☐ F |
| 7 | Problems with medical records lie at the root of a small proportion of adverse incidents | ☐ T | ☐ F |
| 8 | 'Deleted' information on second-hand computer can never be recovered from the hard drive | ☐ T | ☐ F |

INSTRUCTIONS: 1. Go to www.media24medac.co.za/ 2. Click the tab labelled 'Register Online' in the grey strap. 3. Complete the form and click 'Apply'. 4. You will receive an email with your username and password. 5. Login at 'Secure section login'. 6. Within the secure section, complete the applicable ethics article questionnaire. 7. Print certificate certifying CPD points achieved.