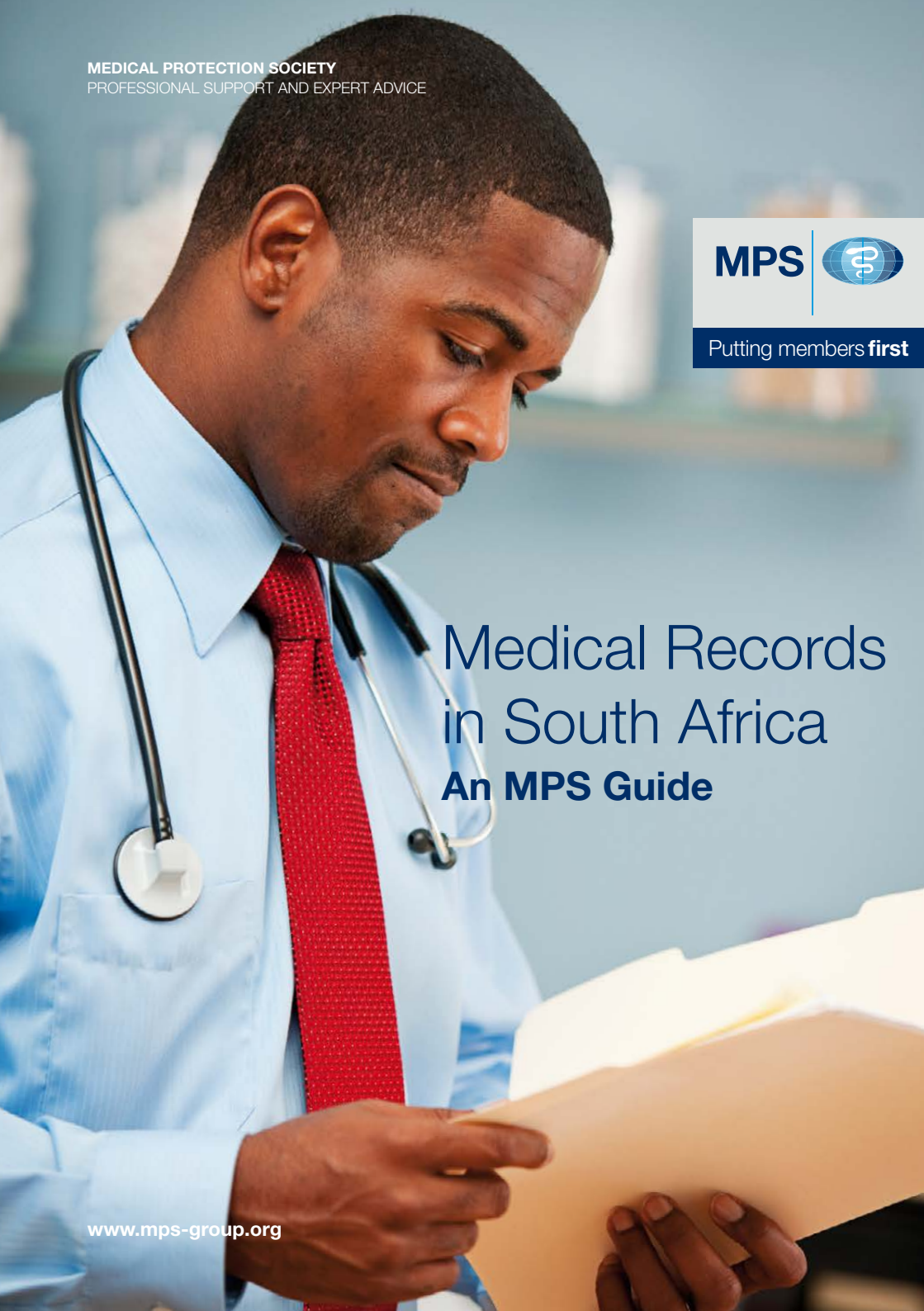

MEDICAL PROTECTION SOCIETY
PROFESSIONAL SUPPORT AND EXPERT ADVICE
MPS
Putting members first
Medical Records in South Africa
An MPS Guide
www.mps-group.org

Contents

Important – please note

Due to the dynamic nature of medical law we suggest that you access our website at www.mps-group.org for the most up-to-date information. June 2014.

First edition published in 2011
This updated and revised edition first published in 2014

Review date June 2016

Cover image: © iStockphoto.com/sjlocke

This booklet was produced as a resource for MPS members in South Africa. It is intended as general guidance only. For more specific practical advice and support with medicolegal issues that may arise, please contact MPS.

MPS is the world's leading protection organisation for doctors, dentists and healthcare professionals. We protect and support the professional interests of more than 290,000 members around the world. Our benefits include access to indemnity, expert advice and peace of mind. Highly qualified advisers are on hand to talk through a question or concern at any time.

Our experts assist with the wide range of legal and ethical problems that arise from professional practice. This includes clinical negligence claims, complaints, medical and dental council inquiries, legal and ethical dilemmas, disciplinary procedures, inquests and fatal accident inquiries.

Our philosophy is to support safe practice in medicine and dentistry by helping to avert problems in the first place. We do this by promoting risk management through our workshops, E-learning, clinical risk assessments, publications, conferences, lectures and presentations.

MPS is not an insurance company. All the benefits of membership of MPS are discretionary as set out in the Memorandum and Articles of Association.

Introduction

Good quality medical records are an essential component of safe and effective healthcare. Their main function is to facilitate continuity of care, but there are also many secondary uses they are put to. This booklet concentrates on the clinical and medicolegal aspects of keeping medical records, and on the related and important issues of confidentiality and security. It is divided into two parts.

Part 1 addresses the quality and accessibility of records, crucial factors in the safe and effective provision of healthcare services.

Part 2 deals with the legislative, regulatory and practical aspects of third-party disclosures and protecting patient records from loss, damage and unauthorised access.

iStockphoto.com/InCommunicado

Part 1 – Quality and accessibility

Quality

Adequate medical records enable you or somebody else to reconstruct the essential parts of each patient contact without reference to memory. They should therefore be comprehensive enough to allow a colleague to carry on where you left off.

Poor-quality medical records are not only a major cause of iatrogenic injuries, they also make it difficult to defend a clinical negligence claim or an HPCSA disciplinary inquiry; it is axiomatic that poor note-keeping is evidence of poor clinical practice. The common problems listed in Box 1 are all-too-frequent reoccurring themes in MPS case files.

Good medical records can be characterised as:

- Comprehensive
- Contemporaneous
- Comprehensible and accurate
- Attributable.

iStockphoto.com/adamgryko

Box 1: Common problems

Any of the following may compromise patient safety or lead to medicolegal problems:

- Not recording negative findings
- Not recording the substance of discussions about the risks and benefits of proposed treatments, including no treatment
- Not recording drug allergies or adverse reactions
- Not recording the results of investigations and tests
- Illegible, unsigned or undated entries
- Not consulting the relevant records when seeing a patient
- Making derogatory comments
- Altering notes after the event
- Wrong patient/wrong notes

Comprehensive

To be useful, the medical records should contain all the significant information that members of the healthcare team, or future carers, will need in order to be sufficiently informed about the patient's past and current clinical assessments and treatment and relevant family and social history, lifestyle and beliefs. The HPCSA considers the contents listed in Box 2 as the absolute minimum necessary for each patient's records.

Box 2: Compulsory elements of clinical records

The HPCSA specifies the following minimum information that should be included in a patient's clinical record:

- Personal (identifying) particulars of the patient.
- The bio-psychosocial history of the patient, including allergies and idiosyncrasies.
- The time, date and place of every consultation.
- The assessment of the patient's condition.
- The proposed clinical management of the patient.
- The medication and dosage prescribed.
- Details of referrals to specialists, if any.
- The patient's reaction to treatment or medication, including adverse effects.
- Test results.
- Imaging investigation results.
- Information on the times that the patient was booked off from work and the relevant reasons.
- Written proof of informed consent, where applicable.

HPCSA, *Guidelines on the Keeping of Patient Records* (2008), para 4.

To this we would add, from a medicolegal and risk-management perspective:

- All important positive and negative findings from the consultation with the patient. Information about the presence or absence of certain signs or symptoms at different stages in the course of a patient's illness is not only important for forming a picture of the development of the patient's condition, but can be crucial in defending any future medicolegal challenges (see Box 3).
- Differential diagnosis, including reasons for ruling out (or preferring) a potential diagnosis.
- Details of discussions with the patient about the risks and benefits of proposed treatments, including the risks of no treatment, costs and any information given to them in this regard (eg, patient information leaflets).
- Any advice or warnings given to the patient – not to drive while taking certain medication, for example.
- Arrangements for follow-up tests, future appointments and referrals made.
- Any instructions or advice given to the patient. It is particularly important to make a note of any instructions you give to patients about what to do if their symptoms change, persist or worsen, such as returning for another consultation.

Box 3: The importance of recording findings

An analysis of MPS cases arising from missed diagnosis of meningitis found that, in many of the cases in the sample, the patient was seen by a series of doctors before a diagnosis was made. This can make it difficult to assess the progress of the patient's illness, so good note taking is crucial. Few of the notes in the sample recorded the patient's temperature, pulse rate or a description of the patient's awareness levels. Moreover, they often omitted the negative findings of clinical examinations.

Anthony, S. Don't Get Caught in the Rash Trap, MPS *Casebook* 14(1): 25 (2006).

Contemporaneous

For the sake of good continuity of care, patients' records should be kept as up to date as possible, which means that information should be added to the patient's notes as soon as it becomes available. It is good practice to make a habit of noting information as it arises so that it is not lost if something happens to distract your attention – eg, an emergency, a phone call, or an interruption by a colleague.

Late entries and addenda

If you are making an entry in a patient's records after an event, do not back-date it; you should clearly mark it as a "late entry" using the date and time at which the entry

is actually made, and referring back to the date and time of the event the notes are about. Include the reason why the entry is being made retrospectively.

Any attempt to pass off a late entry as a contemporaneous note could, if discovered, attract serious criticism, including a finding of unprofessional conduct by the HPCSA or censure by the courts. Do not be tempted, if you find yourself facing allegations of negligence, to augment or alter the original contemporaneous notes. This not only amounts to unethical conduct, but will almost certainly make your case difficult to defend. If the plaintiff's solicitors suspect that you have retrospectively altered the records, they can generally find proof of it by employing forensic experts to examine the ink and paper or by examining the audit trail of computerised records.

If you need to add further information relating to a specific situation or event that was recorded in the notes earlier, include it as an addendum. Enter the current date and time and write "Addendum to entry made on [date and time]", followed by the reason for adding an addendum and the information you wish to add.

Comprehensible and accurate

When making notes in a patient's records, a balance must be struck between brevity and comprehensibility. Generally speaking, the briefer the note, the more open to misinterpretation it will be.

On the other hand, no-one in a busy clinical setting has the time either to write or to read lengthy prose, so your notes should be as precise and concise as you can make them. Avoid generalisations and speculation. Stick to the facts and your objective findings. If you are reporting hearsay (eg, a relative's account), use quotation marks and identify the source. Avoid using abbreviations that may not be understood in the context of multidisciplinary care.

It's an obvious point to make, but errors in medical records can have a devastating effect on patients. Something as simple as a mis-placed decimal point, hearsay presented as fact or test results filed in the wrong patient's records can be fatally misleading. There are many reasons for inaccuracies in medical records – all of which are commonplace occurrences – such as being in a hurry, getting distracted, momentary inattention, or not fully understanding what someone is saying. Consequently, it is very easy for inaccuracies to creep into the records; common causes are: not listening attentively when taking a patient's history; relying on memory after an interruption; hasty writing that's illegible; or not checking the identity of the patient before filing reports or writing a note.

There should, therefore, be a constant process of review and verification of records at the point of care. Confirm important information with the patient, especially when you are seeing a patient for the first time. If anything in the records seems unusual or illogical to you, check its validity – don't assume that it's you who is in error! (See Case 1.) Similarly, if you are prescribing medication or intending to carry out a surgical procedure in response to the transcribed results of a lab report or an investigation, check the actual report first if it is available, to make sure that the information in the medical notes is accurate (see Case 3 on page 26).

Alterations

Once an entry has been made in a medical record, it should not be deleted or obliterated, even if it is later found to be erroneous or misleading. If you need to make a correction, use a single black line to cross out the error and then add the amendment and your signature, name (in block capitals) and the date and time.

Checking the patient's identity

One of the main causes of inaccuracies in medical records is that of mistaken identity (see, for example, Case 1). Experts in risk management recommend that healthcare professionals make it their normal practice to check a patient's identity before a consultation, a procedure or administration of medication. The method they recommend is to ask the patient to state their name and date of birth rather than asking for confirmation that they are who you think they are – "Could you tell me your full name please?" rather than "Are you Mrs Okele?".

Reports and test results can also be easily filed in the wrong patient's records, especially if the patients share the same name, so it is important to double check that other details such as date of birth or an ID number match those on the cover of the records.

Attributable

If you write anything in a patient's records, the HPCSA says that you must sign it and write your name in block capitals.[1] You should also record the date and time and, in the case of hospital records, your bleep or phone number.

Accessibility

A common cause of adverse incidents is lack of access to critical information. This may be because the patient's records were not available at the time, or (more commonly) because the needed information was lost in voluminous casenotes.

Medical records nowadays include a wide variety of documents generated on – or on behalf of – all the health professionals involved in patient care. Any communication related to a patient's clinical condition and care belongs in the healthcare record.

Given the amount of information contained in the average medical record, it is important not only to file information chronologically in the correct section of the case notes, but to extract and highlight any crucial information, such as allergies, sickle-cell status, special drug needs, etc on the summary sheet and/or the cover. Record significant results of tests and investigations in the progress notes and pass on verbally and in writing any significant or critical information when handing over patient care to a colleague.

When writing up your notes, try to organise the information systematically and use headings, etc to make it easier both for you and your colleagues to quickly pick out relevant information. The POMR-SOAP system, though not ideal, has the advantage of imposing a logical, easy-to-follow structure to the medical record. A problem list acts as a quick guide to clinicians seeing a patient for the first time (see Box 4).

If you are hand writing notes, be careful to write legibly and in non-erasable ink. Indecipherable scrawlings are no use to your colleagues. At best, they are valueless if they cannot be understood; at worst, they can be misinterpreted, resulting in avoidable harm to patients. There have been numerous adverse incidents caused purely by mis-read orders and prescriptions, for example.

Box 4: POMR and SOAP

The basic components of the POMR (Problem Oriented Medical Record) are:

1. Data Base – History, Physical Exam and Laboratory Data
2. Complete Problem List
3. Initial Plans
4. Daily Progress Note
5. Final Progress Note or Discharge Summary

Steps 1, 2 and 3 are completed by the admitting physician.

Each problem on the problem list is numbered. The problem list is placed at the front of the case notes.

Daily Progress Notes (step 4) are made on separate pages for each condition on the problem list using SOAP:

Subjective – what the patient says

Objective – what you detect – examination and test results

Assessment – your conclusions

Problem list and **P**lan – management and follow up

iStockphoto.com/VisualField

Standards

Your organisation might have set standards that you are expected to meet regarding the content and structure of medical records. If not, or if you are in private practice, you should refer to guidance developed by relevant professional bodies and associations in South Africa. Alternatively, you might find it useful to refer to national standards set in other countries (see the Resources section on page 32). While there are variations between them, all published standards share the following features:

1. All continuation sheets for progress notes should be labelled with the patient's name and at least one other form of identification, such as a hospital number.
2. Entries and reports should be kept in chronological order.
3. Entries in the notes should be legible and signed, with the name and designation of the author printed in block capitals, along with the date and time.
4. An entry should be made in the medical record on each occasion that a patient is seen by a doctor. In the case of hospital patients, the patient should be seen by a doctor a specified minimum number of times a week.
5. Each record entry should identify the most senior clinician present at the time.

Abbreviations

Abbreviations are commonly used in medical records but can be misinterpreted and lead to mistakes in diagnosis or management. So the rule is, when in doubt, write it out – in full. Sarcastic and derogatory abbreviations have no place in medical records – acronyms like FAS (Fat and Stupid) are gratuitously offensive and sure to destroy any therapeutic relationship if the patient discovers their meaning.

Discharge summaries

Section 10 of the National Health Act 2003 states that all healthcare providers must supply patients with discharge reports. At the bare minimum, these should contain the following information:

- The health service rendered
- The patient's prognosis
- The need for follow-up treatment.

It is also advisable to include information about medication and any relevant warnings and advice for the patient and/or the patient's GP.

Records management

Good records management makes everybody's life easier and facilitates continuity of care, reducing the risk of adverse incidents through misplaced or untraceable records. Problems with medical records – lack of accessibility, poor-quality information, misinformation, poorly organised notes, mis-filing, and many others – are known to lie at the root of a high proportion of adverse incidents.

For the sake of efficiency and safe practice, every healthcare organisation should have a records management policy in place, and this should be regularly reviewed and updated to keep pace with technological advances and legislative requirements. The international standard for records management – ISO/IEC 15489:2001 – Information and Documentation: Records Management – has been adopted as a national standard in South Africa (SANS 15489:2004) and can be purchased from the South African Bureau of Standards (see the Resources section on page 32). The legislative requirements for an acceptable records management policy are broadly set out in sections 19(1) and (2) of the Protection of Personal Information Act No 4 of 2013.

iStockphoto.com/spxChrome

Part 2 – Disclosure and security

Confidentiality

Confidentiality is usually thought of as an ethical issue. It is, but it is also a legal obligation:

- Employed healthcare workers are usually bound by a confidentiality clause in their contracts. There is a common-law contractual duty to preserve professional confidence.
- There is a common-law duty to preserve professional confidence.
- The Constitution guarantees citizens the right to privacy, including the right not to have the privacy of their communications infringed.[2]
- The National Health Act makes it an offence to divulge information about health service users without the user's consent. The only permissible exceptions are when the law or a court order requires disclosure, or if non-disclosure would represent a serious threat to public health. (However see the HPCSA's guidelines in booklet 10 paragraph 9.3 which allows for disclosures to be made that may assist in the prevention or detection of a crime that will put someone at risk of death or serious harm).[3]
- In terms of the Protection of Personal Information Act all employers and all employees are legally obliged to treat all personal information concerning all patients, including their health information, as private and confidential.

iStockphoto.com/mrloz

The obligation of confidentiality goes beyond undertaking not to divulge confidential information; it includes a responsibility to make sure that all records containing patient information are kept securely.

Confidential records should not be left where other people may have casual access to them and information about patients should be sent under private and confidential cover, with appropriate measures to ensure that it does not go astray.

Patients should be informed about the kind of information being held about them, how and why it might be shared, and with whom it might be shared. Patient information leaflets are a convenient way of notifying patients about this, but they are not sufficient in themselves. Bear in mind that few patients will bother to read the leaflets, and some may not be able to read them. It is especially important to understand that with the advent of the Protection of Personal Information Act patients are vested with the right that their personal information will always be treated as confidential. It is not recommended that users be required to agree to a general waiver of their rights to confidentiality. If you intend to use a patients' personal information for purposes other than their immediate care, or to share it with non-medical agents such as social workers, or to use it for research purposes, you must obtain the patient's consent to hold, process and use the personal information for that particular additional purpose.

Confidentiality is not an absolute obligation – there are circumstances in which disclosure is permissible or even mandatory. Disclosures not authorised by patients are the exception and should only be made after careful and due consideration.

Professional ethics

Confidentiality is considered to be central to the trust between doctors and patients and doctors are held responsible by their professional bodies for protecting personal information that patients share with them. An unjustifiable breach of confidentiality is taken very seriously by the HPCSA; its booklet, *Confidentiality: Protecting and Providing Information* (2008), sets out detailed guidance on the circumstances in which patient information can be disclosed to third parties. The principles that should be applied are listed in Box 5 overleaf.

Statutory obligations

The National Health Act 2003 not only obliges all healthcare establishments to create and maintain a health record for every user of the establishment, but also enjoins them to respect patient confidentiality and specifies the circumstances in which patient records can be accessed.

Section 14 states that information relating to a health service user's health status, treatment or stay in a health establishment may only be disclosed with the user's written consent, or in compliance with a court order or a law, or if non-disclosure represents "a serious threat to public health".

Box 5: HPCSA principles of confidentiality

1. Patients have a right to expect that information about them will be held in confidence by health care practitioners. Confidentiality is central to trust between practitioners and patients. Without assurances about confidentiality, patients may be reluctant to give practitioners the information they need in order to provide good care.
2. Where health care practitioners are asked to provide information about patients, they should:

2.1 Seek the consent of patients to disclosure of information wherever possible, whether or not the patients can be identified from the disclosure; Comprehensive information must be made available to patients with regard to the potential for a breach of confidentiality with ICD10 coding.

2.2 Anonymise data where unidentifiable data will serve the purpose;

2.3 Keep disclosures to the minimum necessary.

3 Health care practitioners must always be prepared to justify their decisions in accordance with these guidelines.

HPCSA, *Confidentiality: Protecting and Providing Information* (2008), para 4.

Sections 15 and 16 cover access to records. It says that healthcare workers with access to a user's health records may disclose information "for any legitimate purpose within the ordinary course and scope of his or her duties where such access or disclosure is in the interests of the user". They may also, with the authorisation of the patient concerned, examine health records in the context of delivering treatment.

There are other statutes that include confidentiality clauses regarding particular types of medical information (see Box 6).

iStockphoto.com/drflet – adapted

Box 6: Legislation stipulating confidentiality requirements for certain types of medical information

National Directives and Instructions on Conducting a Forensic Examination on Survivors of Sexual Offence Cases in Terms of the Criminal Law (Sexual Offences and Related Matters) Amendment Act, 2007, Directives 3 and 5.

All results of HIV tests conducted on alleged sexual offenders under this Act must be kept in a locked cupboard accessible only by the head of the health establishment. The results should be given, in a sealed envelope, only to the Investigating Officer, who will, in turn, pass sealed duplicates to the alleged offender and the survivor. A copy of the results must be kept by the health establishment which may, if applicable, make them available to the prosecutor in the event of court proceedings relating to the alleged sexual offence.

Access to the confidential information contained in the J88 form is legally privileged while a police investigation is underway but may be disclosed to the defence lawyer with the consent of the police investigator and the public prosecutor if he or she has obtained a court order.

Choice on Termination of Pregnancy Act, 92 of 1996, section 7.

Records of termination of pregnancy must be made by the practitioner and the person in charge of the facility. The person in charge of the facility must notify the Director-General within one month of the termination, but without including the name or address of the woman concerned. “The identity of a woman who has requested or obtained a termination of pregnancy shall remain confidential at all times unless she herself chooses to disclose that information.”

Children’s Act, 35 of 2005, sections 12, 13, 133 and 134

“Every child has the right to confidentiality regarding his or her health status and the health status of a parent, care-giver or family member, except when maintaining such confidentiality is not in the best interests of the child.”

In addition, the Act specifies that information about a child’s virginity, HIV status and contraceptive use should not be divulged without the child’s consent. In the case of HIV status, the exception is if the child is below the age of 12 and lacks the maturity to understand the implications, in which case the parent or care-giver, a child protection organisation or the person in charge of a hospital may consent to disclosure on his or her behalf.

Where allowing access might be permissible

Situations can arise in which it is justifiable to disclose a patient's medical records to a person other than the patient. In some cases, you might have a statutory duty to share certain information – such as reporting notifiable diseases or disclosing information concerning the commission of offences that may assist the police in the prevention and detection of a serious crime – but in these cases it is unlikely that you will also need to provide access to the medical records themselves.

There are other circumstances, however, where you might need to allow access to part or the whole of a patient's medical records. Each situation must be assessed individually to determine whether disclosure is appropriate in the circumstances. It is essential that the reasons behind any decision to provide a third party with access to a patient's records be comprehensively documented.

Disclosure with patient consent

The first and most obvious exception to the rule of confidentiality is disclosure made with the patient's consent. Insurance companies, employers and people involved in legal proceedings frequently request information about patients. Any disclosure must be with, and limited to, the authority provided by the patient. If this is not forthcoming, no information may be provided. An authority provided by a patient should not constitute a general waiver of confidentiality. An authority should specify the purpose of the disclosure, who may make the disclosure and to whom the disclosure may be made.

Within a healthcare team

Patient care is usually team based and access to patient information is crucial for the safe delivery and continuity of care. The HPCSA states that sharing patient information within a team delivering care to that patient is permissible with the patient's consent. This includes sharing information with professionals not regulated by the HPCSA.[4] Consent can be assumed if a patient agrees, for example, to his doctor referring him to a specialist.

Most patients are aware that information about them needs to be shared among the healthcare professionals delivering care, but they may not know that they have a right to ask for certain information to be withheld. They should be informed of this (via leaflets, notices and verbally) and, if they ask for information about them to be kept confidential, this should be respected.

The sharing of information within the team should be on a need-to-know basis, depending on the role the member of staff has in the patient's care.

Sharing information about HIV status

The status of HIV positive patients should always be treated as highly confidential (see the HPCSA's guidelines in Box 7). Your medical records system should,

therefore, include a means of "sealing" highly sensitive information that can only be accessed by specified individuals.

Sharing information within the healthcare team about a patient's HIV status is only permissible if the patient has given consent or if it is clinically indicated.

Box 7: HPCSA guidelines on patients' HIV status

1. Ethics, the South African Constitution (Act 108 of 1996) and the law recognise the importance of maintaining the confidentiality of the HIV status of a patient.
2. The test results of HIV positive patients should be treated with the highest possible level of confidentiality.
3. Confidentiality regarding a patient's HIV status extends to other health care practitioners. Other health care professionals may not be informed of a patient's HIV status without that patient's consent unless the disclosure is clinically indicated. For treatment and care to be in the best interests of the patient, the need for disclosure of clinical data (including HIV and related test results), to health care practitioners directly involved in the care of the patient, should be discussed with the patient.
4. The decision to divulge information relating to the HIV status of a patient must always be done in consultation with the patient.
5. The report of HIV test results by a laboratory, as is the case with all laboratory test results, should be considered confidential information. A breach of confidentiality is more likely to occur in the ward, hospital or health care practitioner's reception area than in the laboratory. It is, therefore, essential that health care institutions, pathologists and health care practitioners formulate a clear policy as to how such laboratory results will be communicated and how confidentiality of the results will be maintained.

HPCSA, *Ethical Guidelines for Good Practice with Regard to HIV* (2008), para 5.

iStockphoto.com/spxChrome

The HPCSA states: "In the management of an HIV positive patient it is important that the health care practitioner gives due consideration to other health care professionals who are also involved in the management of the same patient (eg where necessary, and with the patient's consent, informing them of the HIV status of the patient)."[5]

Disclosure in the public interest

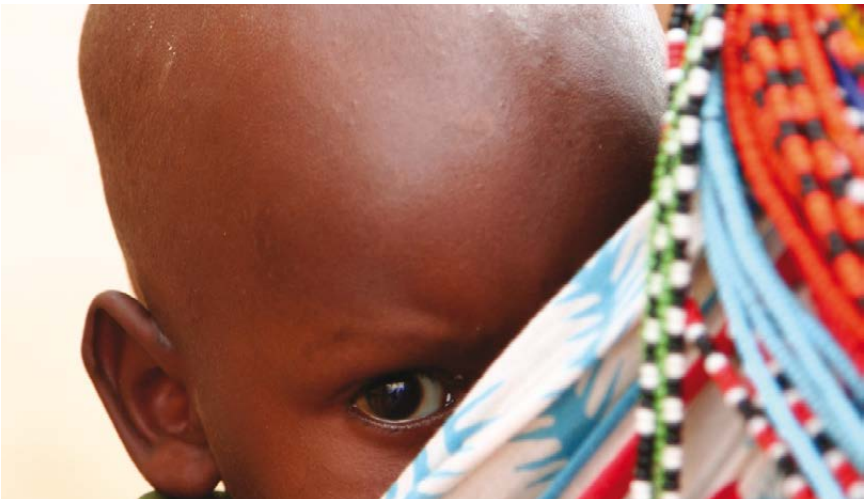
The National Health Act makes an exception to the rule of confidentiality if non-disclosure of a patient's personal health information would pose a serious threat to public health.

HPCSA guidance states that, for disclosure to be justified, the risk of harm to others must be serious enough to outweigh the patient's right to confidentiality. If you judge that this is the case, you should attempt (if it is safe and appropriate) to obtain the patient's consent first, but should go ahead with disclosure to the appropriate authorities if this is not forthcoming.[6]

Carefully document the reasoning beside your decision to disclose, together with details about any discussions you may have had with colleagues in the course of your decision-making.

Protection of vulnerable patients

If you have reason to suspect that a child or adult lacking capacity is being neglected or abused, you must act in the patient's best interests by reporting your concerns to a responsible person or statutory agency.[7] You should try to obtain the patient's consent first, but if this is not forthcoming, the matter should still be reported (preferably with the patient's knowledge).



iStockphoto.com/michieldenijs

Should you on reasonable grounds conclude that a child has been abused in a manner causing physical injury, or has been sexually abused or has been deliberately neglected, you must report that conclusion in the prescribed form to a designated child protection organisation, the provincial department of social development or a police official (see Section 110(1) of the Children's Act 38 of 2005). The HPCSA recommends informing the child's parents first, unless you judge that this would not be in the child's interests.[8]

It is important that you carefully document your reasons for making a disclosure in these circumstances.

Requests for access

The Promotion of Access to Information Act 2000 gives everyone the right of access to records held by either public or private bodies for legitimate purposes. In the latter case, people should be allowed access to "any information that is held by another person and that is required for the exercise or protection of any rights".[9] This includes access to health records.

Either the patient him/herself, or someone authorised to act on the patient's behalf, can request access; ordinarily the request itself is made in writing and should be responded to within 30 calendar days.

The only ground for refusing access is if disclosure "to the relevant person" (ie, the patient or the person requesting access on the patient's behalf) "might cause serious harm to his or her physical or mental health, or well-being".[10]

The Act sets out detailed conditions in this section. Essentially, it states that if the person tasked with deciding whether to grant access or not (the "information officer") thinks that disclosure might result in serious harm to the relevant person, he/she must consult with a healthcare practitioner nominated by the relevant person. If the relevant person is under the age of 16, the nomination must be made by a person with parental responsibility. If the patient lacks capacity, the nomination must be made by a person appointed by the court to manage the patient's affairs.[11]

If the nominated healthcare practitioner, after viewing the records, agrees that disclosure would be likely to cause serious harm to the relevant person as outlined above, the information officer may still allow access to the records if he/she is satisfied that adequate counselling arrangements have been made "to limit, alleviate or avoid" such harm. The appointed counsellor must be given access to the record before access is allowed to the requester.[12]

Relatives

Relatives have no automatic right of access to an adult patient's records. If the patient lacks the mental capacity to consent to disclosure, a relative may apply for access to the medical records under the Promotion of Access to Information Act.

Parents and guardians

The parents of a child under the age of 12 should be given access to the child's medical records if they request it, but bear in mind that if the child has had a termination of pregnancy, this information should remain confidential unless the child consents to its disclosure.

If a child is aged 12 or more, and has the maturity to understand the implications, you will need to secure the child's consent before disclosing his or her medical record.

Deceased patients

The principle of confidentiality extends beyond a patient's death. Generally speaking, information should only be disclosed to third parties with the consent of the deceased's next of kin or executors, but there are exceptions to this rule – information can be disclosed if it is required by an inquest magistrate, for example.

In addition to obtaining the authority of the deceased's next of kin or executor, the HPCSA's advice is to consider the circumstances when deciding whether to accede to a request for information and to consider the effect that disclosure is likely to have on the deceased patient's partner or family.[13]

Court orders

You should comply with a court order to disclose health records. Even if you have concerns about disclosing the records, you should still comply with the order and attach a covering letter to the judge or the registrar of the court describing your concerns. Generally, compliance with a court order should be considered mandatory, but in exceptional circumstances, if you have concerns, it may be appropriate to seek advice from MPS. The mere threat of a court order is not sufficient authority to disclose.

The police

In general, the police have no more right of access to confidential information than anybody else, except in the following circumstances:

- The patient has given consent to the release of information.
- The information is needed in compliance with a court order.
- A written directive has been issued by a judge or a magistrate in terms of section 205(1) of the Criminal Procedure Act 51 of 1977 to disclose information.
- The public interest in disclosing information outweighs the public interest in preserving patient confidentiality. This is not a decision to be taken lightly, so it is best to consult with an MPS medicolegal adviser or a colleague when weighing these competing interests.

Solicitors

Solicitors may request a copy of a patient's medical records in relation to a claim. If the solicitor is acting for the patient, you should not release the records without the patient's (or a legally recognised proxy's) consent. If the solicitor is acting for a third party, you should not release the records unless the request is made in terms of the Promotion of Access to Information Act and the information requested is

(a) About an individual who has given written consent to the requestor or you for the disclosure to be made;

(b) Already publically available;

(c) Information which belongs to a class of information that would or might be made available to the public in any event;

(d) About an individual's physical or mental health, or wellbeing who is under the care of the requester and who is under the age of 18 or is incapable of understanding the nature of the request and giving access would be in the individual's best interests;

(e) About an individual who is deceased and the requester is the next of kin or the solicitor is making the request with the consent of the deceased's next of kin.

(See Chapter 4 section 63(1) and (2) to the Promotion of Access to Information Act 2 of 2000.)

iStockphoto.com/brennanwesley

ICD-10 Coding

Previously the HPCSA "strongly recommends" getting a patient's written consent before disclosing information to a medical scheme. Such written consent can be a "once-off" applying to patient contact concerning the same or a similar clinical condition, but subject to verbal reminders and confirmation (which should be documented in the patient's records). When the patient presents with a new condition, it will be necessary to obtain new written consent. The 2008 booklet makes no such recommendation.

The patient's consent must be fully informed, based on a full and frank discussion about who will be accessing the information and for what purpose, and the implications of disclosure v non-disclosure. The patient should be informed that the medical scheme has the discretion to reject claims with a U 98.0 code (Patient refused to disclose clinical information).[14]

Doctors who provide services that do not involve direct contact with the patient (pathologists, for example) should confirm with the commissioning doctor that the patient has consented to his/her medical information being accessed and to clinical information being disclosed to his/her medical scheme.

Teaching and publishing

Teaching and research

The National Health Act states that the use of identifiable information in medical records can only be used for study, teaching or research if it has been authorised by the patient and the head of the health establishment concerned and the relevant health research ethics committee. The Protection of Personal Information Act states that no identifiable personal information may be used for study, research or teaching unless the patient has authorised the disclosure for that particular purpose.

Publishing case reports, photographs or other images

The HPCSA says that a patient's express consent must be obtained before publishing case reports, photographs or other images in media that the public can access. This rule applies regardless of whether the patient can be identified or not.[15]

Research and audit

If you are conducting your own clinical audit based on your patients' personal information including medical records, you must obtain the patient's authority to hold and process the information for that purpose. If it is necessary to include information that could be used to identify individual patients, you must always first secure the patient's express consent.

Management and financial audit

Files relating to administration should be kept separately from the patient's medical records. Wherever possible, records used for financial audit by a third party (such as a medical scheme) should be anonymised and provided in accordance with the guidance issued by the HPCSA in its booklet, *Confidentiality: Protecting and Providing Information*. Disclosure of information should be limited to the relevant parts of the record.[16]

Security

Statutory requirements

The National Health Act 2003 obliges healthcare providers to create and maintain a medical record for each of their patients. Moreover, it requires them to introduce control measures to restrict access to those records or the records' storage facility to authorised personnel (see Box 8 overleaf).

The Protection of personal Information Act obliges you to secure the integrity and confidentiality of personal information by taking appropriate, reasonable technical and organisational measures to prevent loss of, damage to or unauthorised destruction of or unlawful processing or access to personal information. Appropriate and reasonable measures will include identifying all reasonably foreseeable internal; and external risks to personal information under your control, establishing and maintaining appropriate safeguards against the risks so identified, verifying that the safeguards have been effectively implemented and ensuring that the safeguards are continually updated to meet your operational requirements (see section 19(1) and (2) to the Protection of Personal Information Act 4 of 2013).

The key to safeguarding your patients' confidential information is a sensible records management policy incorporating strong security controls. The policy should apply to both computerised and manual records and include measures to protect the physical integrity of the records (see Appendix 3).

For comprehensive guidance on all aspects of records security, the ISO standard ISO/IEC 27002: 2005 – covers everything you need to know (and more) about averting threats to the confidentiality, integrity and availability of your records. It offers a menu of hundreds of suggested controls for a wide range of 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/IEC 27002 covers all manner of threats to records, which might be bewildering for a non-expert in this field. Fortunately, a recently published standard aimed specifically at the health sector and drawing on ISO/IEC 27002 content has come to the rescue. ISO 27799: 2008 – Health Informatics: Information Security Management in Health – contains all the relevant guidance in ISO/IEC 27002 as it relates to the healthcare sector.

Box 8: NHA on protection of health records

Section 17 of the National Health Act makes the following provisions for the protection of health records:

17. (1) The person in charge of a health establishment in possession of a user's health records must set up control measures to prevent unauthorised access to those records and to the storage facility in which, or system by which, records are kept.

(2) Any person who fails:

(a) to perform a duty imposed on them in terms of subsection (1);

(b) falsifies any record by adding to or deleting or changing any information contained in that record;

(c) creates, changes or destroys a record without authority to do so;

(d) fails to create or change a record when properly required to do so;

(e) provides false information with the intent that it be included in a record:

(f) without authority, copies any part of a record;

(g) without authority connects the personal identification elements of a user's record with any element of that record that concerns the user's condition, treatment or history;

(h) gains unauthorised access to a record or record-keeping system, including intercepting information being transmitted from one person, or one part of a record-keeping system, to another;

(i) without authority, connects any part of a computer or other electronic system on which records are kept to:

(i) any other computer or other electronic system; or

(ii) any terminal or other installation connected to or forming part of any other computer or other electronic system; or

(j) without authority, modifies or impairs the operation of:

(i) any part of the operating system of a computer or other electronic system on which a user's records are kept; or

(ii) any part of the programme used to record, store, retrieve or display information on a computer or other electronic system on which a user's records are kept, commits an offence and is liable on conviction to a fine or to imprisonment for a period not exceeding one year or to both a fine and such imprisonment.

Both these standards can be purchased via the South African Bureau of Standards (see Resources section on page 32).

Access

Section 17 of the National Health Act makes it an offence, punishable by a fine, imprisonment or both, to access or copy patient information without authorisation.

Controls should be put in place to restrict access to records to staff who need to view the records to fulfil their duties. The level of such access should be arranged on a need-to-know basis, if possible. This is easier to organise when the records are held on computer systems, which lend themselves to passwords and degrees of access. Nevertheless, access controls can still be effectively introduced for paper records by implementing rigid protocols determining who may access the records and for what purpose, and backing them up with robust staff training, explicit confidentiality agreements, and limited access to keys and access codes, etc.

Preservation

Although most of us think of security in terms of safeguarding against unauthorised access, there is another important aspect – protecting records from physical damage. Paper records in particular can be easily damaged by moisture, water, fire and insects. And – unlike electronic records – it's not feasible to create up-to-date copies against the chance destruction of the originals. Your paper records are therefore not only vulnerable, but irreplaceable, so it's a good idea to carry out a risk assessment to identify ways in which you can reasonably safeguard their physical integrity. Some of the factors that should be considered in a risk assessment are outlined in Appendix 3.

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

Summary

- Keeping good medical records is essential for continuity of care, especially when many clinicians are involved in a patient's care. Good record keeping is an integral part of good professional practice.
- Records should include sufficient detail for someone else to take over a patient's care, seamlessly, from where you left off.
- Records that ensure continuity of care will also be adequate for evidential purposes, in the event of a complaint, claim or disciplinary action.
- Medical records should be clear, objective, contemporaneous, tamper-proof and original.
- Abbreviations, if used, must be unambiguous and understood by all members of the healthcare team.
- Medical records comprise handwritten and computerised notes, correspondence between health professionals, laboratory reports, x-ray and other imaging records, clinical photographs, videos and other recordings, and printouts from monitoring equipment.
- Medical records are sensitive personal data and must be kept securely to prevent damage and unauthorised access.
- Medical records can usually be shared with other members of the clinical team responsible for clinical management, unless the patient objects.
- Access to records or the information they contain is also permissible in other circumstances but the record holder must always be prepared to justify disclosure.
- Where information from medical records is required for audit and research purposes, consent should be taken from the data subject to process the information for that purpose.
- Any alteration to medical records should be patently apparent to avoid any accusation that there has been an attempt to mislead or deceive.
- Common problems are illegibility of handwritten notes, failing to date and sign them, inaccurate recording of information or insufficient detail.

Case studies

iStockphoto.com/stevecoleccs

Case 1

Two senior doctors doing their rounds in an orthopaedic ward were pleasantly surprised to find that an elderly woman admitted with an undisplaced fractured neck of femur was able to weight-bear and walk with no apparent discomfort. Accordingly, they noted this finding in the patient's record and recommended that she be treated conservatively. This puzzled an intern familiar with the patient; he knew that she had been on bed rest since admission and was experiencing significant pain. It transpired that the two doctors had evaluated the wrong patient – another elderly woman of about the same age.

Based on case report *"Mistaken Identity"*, www.webmm.ahrg.gov October 2008.

Case 2

A woman with Takayasu's arteritis was admitted to hospital with severe abdominal pain. Takayasu's is a rare condition that results in arterial stenoses, which can cause different blood pressure readings in each arm if one arm has more arteritis than the other. This was the case with this patient, who had markedly different blood pressure in her left and right arms. Although this phenomenon was documented in the patient's notes, the information was not transferred either to her charts or her wristband.

An IV infusion of normal saline was started in the patient's left arm to rehydrate her prior to vascular surgery arranged for the following morning.

During the night, a nurse reported to the doctor on call that the patient's systolic blood pressure was only 70mmHg. The doctor, who had not been told about the patient's history of different BP in each arm during the shift handover, ordered norepinephrine, which the nurse (who was also ignorant about the patient's history) administered.

Luckily, the error was discovered the following morning and the order for norepinephrine was discontinued before the patient suffered any ill effects.

Based on case report *"On the Other Hand"*, www.webmm.ahrq.gov May 2007.

Case 3

A woman was admitted to a maternity unit at 39 weeks with vaginal bleeding.

A midwife mistakenly recorded that she was rhesus positive in her medical record; consequently, she was not given Anti-D immunoglobulin. The error came to light two days later when another midwife reviewed the laboratory report in the patient's notes.

Based on case history 10 from National Haemovigilance Office (Ireland) *Annual Report* (2006).

Case 4

A 60-year-old man had been attending a urology clinic twice a year for four years for treatment related to a benign prostatic hyperplasia when his urologist took up a post in another hospital. The new urologist, after briefly reviewing the patient's copious notes (he'd had multiple medical and surgical pathologies over the years), decided that the patient's symptoms had been stable for some time and discharged him from the urology clinic.

Twelve months later, the patient complained of pain in his left loin and haematuria. Renal ultrasound demonstrated a slight hydronephrosis of the left kidney, and also the presence of a ureteric stent. The stent had been inserted by his previous urologist 14 months earlier to protect the left ureter from injury during a left hemicolectomy performed by a general surgeon. The intention had been to remove the stent five to six months after the surgery, but this information had not been passed on to the new urologist. In fact, no mention of the stent had been made in the urology section of the patient's notes.

By this time the stent had become encrusted with stone and had to be removed under general anaesthetic.

Based on case report "Continuity of care", MPS *Casebook* Vol. 17 (1) January 2009

Case 5

A doctor prescribed a transfusion of packed red cells for a patient with an Hb of 7.5g/dl. While the transfusion was in progress, the doctor checked the results of the patient's blood test on the hospital computer and found that her Hb was actually 12.5g/dl. The transfusion was discontinued and the patient suffered no ill effects.

When the error was investigated, they found that a nurse had transcribed a different patient's test results from the computer into the patient's records.

Based on Case History "Unnecessary Transfusion", National Haemovigilance Office (Ireland) *Annual Report* (2006).

Appendix 1

Retention and disposal of records

Retention

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

- Records should be kept for at least 6 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.
- In terms of section 14 of the Protection of Personal Information Act 4 of 2013 records of personal information must not be retained any longer than is necessary for achieving the purpose for which the information was collected and processed. Records should not be retained randomly on an indefinite basis.
- Statutory and regulatory obligations to keep certain types of records for specific periods must be complied with.

HPCSA, *Guidelines on the Keeping of Patient Records* (2008), para 9.

Disposal

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.[17]

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. 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 provide 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.

Appendix 2

Ownership and transfer of records

Ownership

Contrary to what patients may believe, healthcare records generally belong to the establishment that created them. Patients have rights concerning the information contained in their records, but they do not normally own the actual documents or electronic files. The exception is where a patient has paid for records or images.[18]

See the HPCSA's guidance – *Guidelines on the Keeping of Medical Records* – for details about the correct procedures for managing medical records after a practitioner dies or decides to cease practising.

Transferring records

If a patient transfers to another doctor, you may forward a copy of the patient's records to the new doctor, while retaining the original for your own records. These should be disposed of at the end of the retention period in your records management policy (See Retention of medical records in Appendix 1).

Appendix 3

Paper records – environmental risks

Fire

Install chemical fire extinguishers (do not use a sprinkler system as water can be even more damaging than fire). Smoke from fires elsewhere in the building can also do much damage, so make sure that doors are tight-fitting and kept closed. Inflammable liquids kept on the premises should be properly stored, and as far away as possible from the records. Install smoke and fire alarms, preferably a system that connects directly to the local fire service.

Important paper documents should be kept in a fire-proof safe, but do not entrust your computer back-up drive to a fire-proof safe – it can melt. Instead, use secure off-site storage.

Water

Basements are not a good place for archiving records – better to use professional off-site archiving services if you don't have a suitable space for storing inactive files. If you are in a flood-prone area, store records above floor level. Think also about the risks from leaking roofs and plumbing problems. If you have sprinklers in areas that house computers, put waterproof covers on the computers before going home at night.

Gravity

Paper records can be very heavy, so get an engineer to check that the floor of your records room can carry the load.

Insects and vermin

Have regular inspections and control measures carried out by experts to keep damaging insects and rodents at bay.

Poor building maintenance

Dangerous wiring, gas leaks, plumbing problems, leaking roofs and damp walls can all cause damage to both paper and electronic records. A regular building maintenance programme can help to reduce the risk from these elements.

Appendix 4

Resources

South African Bureau of Standards (SABS)
www.sabs.co.za

Postal address: Private Bag X191, Pretoria 0001
Tel: 012 428 6883
Fax: 012 428 6928
email sales@sabs.co.za

Health Professions Council of South Africa
www.hpcsa.co.za

Guidelines for the Management of Patients with HIV Infection or Aids, Booklet 8 (July 2002)

Confidentiality: Protecting and Providing Information (second edition), Booklet 11(May 2007)

Guidelines on the Keeping of Patient Records (second edition), Booklet 15 (May 2007)

Royal College of Physicians, London
www.rcplondon.ac.uk

Generic Medical Record Keeping Standards (August 2007) [12 essential standards]

International Council on Archives
www.ica.org

Principles and Functional Requirements for Records in Electronic Office Environments [Training manuals in three modules]

International Records Management Trust
www.irmt.org

Managing Hospital Records [Module 16 of the Trust's Management of Public Sector Records Study Programme. The material is particularly relevant for hospitals with limited resources.]

ICD-10 National Task Team
www.doh.gov.za/docs/reports/2007/nhis/acknow.pdf

Patient Confidentiality Subcommittee Report (2007)

National Health Act 2003
www.acts.co.za/national_health/index.html

References

1 HPCSA, *Guidelines on the Keeping of Patient Records* (2008), para 5

2 Constitution of the Republic of South Africa 1996, section 14(d).

3 National Health Act 2003, section 14(1).

4 HPCSA, *Seeking Patients' Informed Consent: The Ethical Considerations* (2008), para 18.2.

5 HPCSA, *Ethical Guidelines for Good Practice with Regard to HIV* (2008), para 4.5.

6 HPCSA, *Confidentiality: Protecting and Providing Information* (2008), para 9.3.1.

7 HPCSA, *Confidentiality: Protecting and Providing Information* (2008), para 9.4.2.

8 HPCSA, *Confidentiality: Protecting and Providing Information* (2008), para 9.4.2.2.

9 Promotion of Access to Information Act 2 of 2000, section 9(ii).

10 Promotion of Access to Information Act 2 of 2000, section 61(1)

11 Promotion of Access to Information Act 2 of 2000, section 61(2)

12 Promotion of Access to Information Act 2 of 2000, section 61(3)

13 HPCSA, *Confidentiality: Protecting and Providing Information* (2008), para 9.5.1.

14 HPCSA, *Seeking Patients' Informed Consent: The Ethical Considerations* (2008), para 18.

15 HPCSA, *Confidentiality: Protecting and Providing Information* (2008), para 9.1.4.

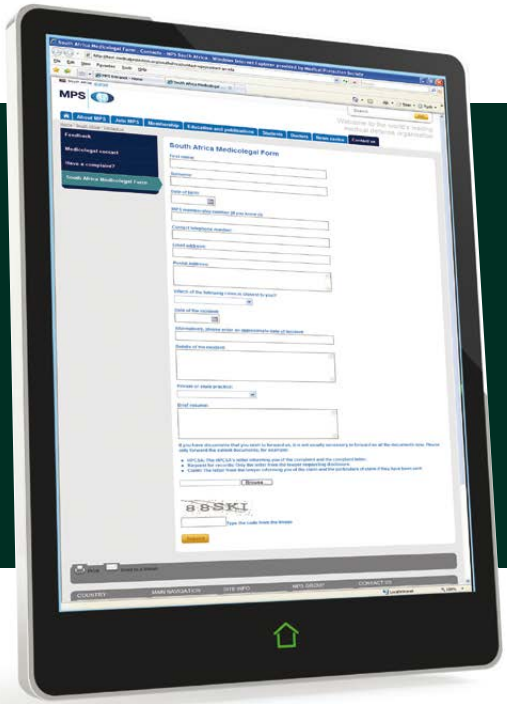
16 HPCSA, *Confidentiality: Protecting and Providing Information* (2008), para 9.1.2.

17 Electronic Communications and Transactions Act 25 of 2002

18 HPCSA, *Guidelines on the Keeping of Medical Records* (2008), para 10.2

MEDICAL PROTECTION SOCIETY
PROFESSIONAL SUPPORT AND EXPERT ADVICE

Helping members in **South Africa**
for more than **50 years**



MPS

Putting members **first**

Medicolegal advice request form now online for MPS members in South Africa

www.mps-group.org/za-mla

To help us provide you with assistance as quickly as possible please use the medicolegal contact form on our website.

The form is secure and confidential – allowing you to give us your MPS membership details and a brief explanation of an incident. The information you provide comes directly to MPS and the receipt of the form will be acknowledged by email immediately.

On the next working day we will open a new case for you and we will contact you as soon as possible to discuss the matter further.

If you need immediate advice please call our toll free telephone: **0800 982 766**.

MPS ONLINE REPORTING FORM
www.mps-group.org/za-mla

You can scan this quick code to access the incident form on your mobile device

For questions about your MPS membership you can continue to call **0800 225 677** or email your query to **mps@samedical.org**

To find out more visit **www.mps-group.org**

MPS0000: 06/12

MEDICAL PROTECTION SOCIETY
PROFESSIONAL SUPPORT AND EXPERT ADVICE

MPS Putting members first

www.mps-group.org

How to contact us

South Africa medicolegal advice

www.mps-group.org/za-mla

To help us to provide you with assistance as quickly as possible please use the medicolegal contact form on our website.

The form is secure and confidential – allowing you to give us your MPS membership details and provide a brief explanation of an incident. The information you provide comes directly to MPS and the receipt of the form will be acknowledged by email immediately.

On the next working day we will open a new case for you and we will contact you as soon as possible to discuss the matter.

T 0800 982 766 (toll-free within SA)
E medical.rsa@mps-group.org

In the interests of confidentiality please do not include information in any email that would allow a patient to be identified.

South Africa membership enquiries

Ian Middleton
T 0800 118 771 (toll-free within SA)
E mps@global.co.za

Alika Maharaj
T 083 277 9208 (cell phone)
E mps@iburst.co.za

South African Medical Association
T 0800 225 677 (toll-free within SA)

MPS0948:06/14