
MEDICAL PROTECTION SOCIETY
PROFESSIONAL SUPPORT AND EXPERT ADVICE
MPS
Putting members first
Medical records in Ireland
An MPS Guide
www.medicalprotection.org/ireland

Contents

Important – please note

Due to the dynamic nature of medical law we suggest that you access our website at www.medicalprotection.org/ireland for the most up-to-date information. September 2013

Revised edition published December 2010, June 2012, September 2013

Review date September 2015

Cover image: © iStockphoto.com/Rubberball

This booklet is published as a resource for MPS members in Ireland. It is intended as general guidance only. MPS members are always welcome to telephone our medicolegal advice line – 1800 509 441 – for more specific practical advice and support with medicolegal issues that may arise.

The Medical Protection Society is the leading provider of comprehensive professional indemnity and expert advice to doctors, dentists and health professionals around the world.

We are a mutual, not-for-profit organisation offering more than 280,000 members help with legal and ethical problems that arise from their professional practice. This includes clinical negligence claims, complaints, medical council inquiries, legal and ethical dilemmas, disciplinary procedures, inquests and fatal accident inquiries.

Fairness is at the heart of how we conduct our business. We actively protect and promote the interests of members and the wider profession. Equally, we believe that patients who have suffered harm from negligent treatment should receive fair compensation. We promote safer practice by running risk management and education programmes to reduce avoidable harm.

MPS is not an insurance company. The benefits of membership are discretionary – this allows us the flexibility to provide help and support even in unusual circumstances.

Introduction

Good clinical records are a prerequisite of delivering high-quality, evidence-based healthcare, particularly where a number of different clinicians are contributing simultaneously to patient care. Everyone involved in a patient's clinical management should have access to the information they need – otherwise, duplication of work, delays and mistakes are inevitable.

Records may be held electronically or manually, or a mixture of both. Some healthcare professionals – for example physiotherapists, occupational therapists, speech therapists and psychologists – often maintain separate departmental records, sometimes (but not always) copying important information relevant to others into the main hospital record. But in any event, a patient's clinical record is never a single document. Increasingly, GPs hold their records in computerised form and many hospitals hold a mixture of electronic and paper records. These should be cross-referenced with other files that may exist in various departments.

The information contained in clinical records may also be required for a range of non-clinical uses described below. Clinical records contain sensitive personal data, and keeping them secure from prying eyes or inadvertent disclosure is a legal – as well as a professional – responsibility.

Why keep clinical records?

The main purpose of any clinical record is to provide continuity of care, but medical records are also used for other purposes:

- Administrative and managerial decision-making.
- Meeting current legal requirements, including enabling patients to access their records.
- Assisting in clinical audit.
- Supporting improvements in clinical effectiveness through research.
- Providing the necessary factual base for responding to complaints and clinical negligence claims.

In general, clinical records that contain sufficient information to secure continuity of care will also contain the information required for all other purposes.

In the event of a complaint, clinical negligence claim or disciplinary proceedings, the doctor's defence will in large part depend upon the evidence available in the clinical records. If essential information is missing, found to be inaccurate or indecipherable, cases may be lost when they could otherwise have been won.

Where possible, information used for non-clinical purposes should be anonymised.

Case 1

At six months old, a boy suffered with diarrhoea and vomiting. His GP was called and treatment provided at home. Due to severe dehydration, he became both physically and mentally handicapped. When he was in his 20s, a solicitor suggested investigating the circumstances surrounding the illness and a claim of negligence arose. By this time, the GP had died, leaving only minimal scant medical records of his consultations. In the absence of any robust evidence to the contrary, the claim against the doctor's estate had to be settled.

What are clinical records?

Clinical records include a wide variety of documents generated on, or on behalf of, all the health professionals involved in patient care. This includes:

- Handwritten clinical notes
- Computerised/electronic clinical records
- All personal correspondence (including letters, faxes, text messages and emails) relating to clinical matters, including correspondence sent between hospital and practice
- Scanned records
- Laboratory results
- X-ray films and other imaging records
- Photographs
- Videos and audio recordings
- Printouts from monitoring equipment, particularly in anaesthesia and obstetrics, A&E and ICU
- Consent forms.

What makes good clinical records?

Content

Good clinical records will contain all the information one clinician needs to take over where another left off – or, to put it another way, to allow a clinician to reconstruct a consultation or patient contact without relying on memory. This will include:

- History – relevant to the condition including any positive and negative answers to direct questions
- Examination of the patient
- All systems examined
- All important findings, both positive and negative, with details of any objective measurement such as blood pressure, peak flow, etc
- Differential diagnosis
- Investigations – details of any investigations arranged
- Referral – details of any referral made
- Information – information given to the patient concerning risks and benefits of proposed treatments
- Consent – details of consent given to proposed investigations, treatments or procedures
- Treatment – details of the main doses of drugs, total amount prescribed, any other treatment organised with batch number and expiry date of any medications personally administered
- Follow-up – arrangements for follow-up tests, future appointments and referrals made
- Progress – any further consultations, the patient's current condition, side effects, complications, etc.

That may seem like a daunting list, but it is all important information that someone would have to remember if it is not recorded – and both doctors' and patients' memories are fallible. Many follow-up consultations will be with different members of the team, who will be totally reliant on the clinical records and therefore will need as much information as possible.

The mnemonic **SOAP** (see page 7) is a useful reminder of the essential content you should include.

Box 1: Essential content (SOAP)

- **S**ubjective – what the patient says
- **O**bjective – what you detect – examination and test results
- **A**ssessment – your conclusions – often the differential diagnosis
- **P**roblem list & **P**lan – management and follow up

Case 2

A 26-year-old single woman went to see her GP complaining of blackouts. He referred her to a neurologist, giving a detailed account of the blackouts but not disclosing the medication she was on, which included the oral contraceptive pill. The neurologist started the patient on anticonvulsants. Three months later she conceived. Her claim against both doctors succeeded.

As the GP had failed to alert the neurologist to the fact the patient was taking the oral contraceptive pill, and the neurologist had not asked about medication, both had been in breach of their duty of care, causing the unwanted pregnancy.

Presentation

Content is important, but so is presentation. If the records are unclear, inaccurate or written in such a way that they're difficult to follow, the content might as well not be there; worse than that, it could cause errors and misunderstandings. Good notes therefore have the following attributes:

- **Clear** – both legible and understandable when handwritten. Each entry should be legibly signed with the date and time.
- **Objective** – clinical records should be factual and free from subjective comments about patients or their relatives. Always assume that patients will read their clinical records at some stage.
- **Contemporaneous** – clinical records should be written up at the time of, or as soon as possible after, an event to ensure accuracy. Retrospective entries should be clearly dated, timed and signed, together with an explanation of why it is being written retrospectively.
- **Attributable** – if information has been given to you by someone other than the patient, then you should record who provided the information as well as what they said.
- **Original** – sometimes it is necessary to amend or alter medical records, for example if a factual error has been made. Any correction must be clearly shown as an alteration, complete with the date the amendment was made and the name of the person who made it so there can be no allegation that the alteration was an attempt to deceive anyone into thinking that it is part of the original record. (See Box 2.)

Box 2: HSE guidelines on correcting medical records

19. Records shall not be erased or destroyed but shall be amended if incorrect.

20. Correction fluids shall not be used. The original entry shall remain visible.

21. Deletions or alterations shall be made by scoring out with a single line followed by:
    - Signature (plus name in capitals) and counter signature, if appropriate.
    - Date and time of correct entry.
    - Reason for amendment.

22. Corrections shall be made as close to the original recording as possible.

23. Alterations to prescriptions shall not be permissible. A prescription that is no longer appropriate shall be discontinued and a new prescription shall be written.

National Hospitals Office, *Code of Practice for Medical Records Management* (2007)

Abbreviations

Abbreviations are commonly used in clinical 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. Be aware, too, that patients may, if they access their notes, misinterpret innocuous abbreviations such as SOB (shortness of breath), which most lay people would interpret as an insulting reference to their origins. (See Box 3 for the rules on abbreviations that apply in national hospitals.)

Sarcastic and derogatory abbreviations have no place in clinical records – they are gratuitously offensive and sure to destroy any therapeutic relationship once found out.

Case 3

A 38-year-old woman phoned her GP surgery complaining of back pain and difficulty passing urine. The GP checked her notes and saw a reference to PID, which he interpreted as pelvic inflammatory disease. He concluded that she had another urinary tract infection and wrote a prescription for antibiotics for the patient to collect. In fact PID referred to her recurring problems with a prolapsed intervertebral disc which had now given rise to a cauda equina syndrome and associated pain and urinary symptoms.

Box 3: Use of abbreviations in national hospitals

35. Abbreviations shall not be used. In the event of abbreviations being utilised, only abbreviations approved by the National Hospitals Office may be permitted.

36. All approved abbreviations shall be written in higher case (capital) BLOCK letters and not in a cursive script and/or in lower case.

37. Other than the abbreviations approved by the National Hospitals Office, on each side of each page thefull term shall be used, followed by the abbreviation in brackets. Thereafter the abbreviation may be used on that page.

38. Abbreviations shall not be used on documentation which is used for transfer, discharge or external referral letters.

39. Abbreviations shall not be used on consent forms, death certificates, incident report forms and communications sent from the hospital.

Note: Drug names shall not be abbreviated.

National Hospitals Office, *Code of Practice for Medical Records Management* (2007)

Common problems

All of the following can compromise patient safety or lead to medicolegal problems:

- Not recording negative findings
- Not recording substance of discussions about the risks and benefits of proposed treatments
- Not recording drug allergies or adverse reactions
- Not recording the results of investigations and tests
- Illegible entries
- Not reading the notes when seeing a patient
- Making derogatory comments
- Altering notes after the event
- Wrong patient/wrong notes.

Box 4: HSE guidance on identifying patients

"Before the healthcare professional makes an entry in the patient's healthcare record, s/he shall establish that the record belongs to the patient being attended.

"This shall be done by verifying with the patient and by cross-referencing the patient's wrist band with the healthcare record."

National Hospitals Office, *Code of Practice for Medical Records Management* (2007), p21

Confidentiality of records

Confidentiality may seem a very straightforward principle, but translating principle into practice can be problematic. There are all sorts of situations where it is difficult to know if patient information should be shared or not – with the gardai, for example, or social workers.

Confidentiality is usually referred to as an ethical issue. It is, but it is also a legal principle.

- Healthcare workers are usually bound by a confidentiality clause in their contracts.
- There is a common-law duty to preserve professional confidence.
- There are requirements under the Data Protection Act to keep personal data, including medical records, secure.
- It is a condition of registration to abide by Medical Council guidance, which includes a requirement to respect patient confidentiality.

The duty of confidentiality goes beyond undertaking not to divulge confidential information; it includes a responsibility to make sure that written patient information is 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.

Box 5: Informing patients

A woman complained to the Data Protection Commissioner after she received a letter from researchers asking her some questions about her attendance at the A&E department of a public hospital some months earlier. She had not been told at the hospital that her personal information would be used in this way, but the researchers evidently knew the reason for her visit to A&E.

The hospital argued that it had met its obligations under the DPA by placing a notice about the research in the waiting area of the A&E department. The Commissioner did not agree, however. He pointed out that A&E patients are likely to have their minds on other things and are therefore unlikely "to be alert to matters not relating directly to their condition. In such circumstances there is a special need for the data controller to satisfy itself that any uses of the data which are unlikely to be anticipated by the data subject are fully explained". The hospital should, therefore have brought its intentions to the specific attention of the patient so that she could make an informed choice.

Data Protection Commissioner, Case Study 1/97

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 inform patients – and to let them know that they have the right to withhold consent – if you intend to use their personal information for purposes other than their immediate care, or to share it with non-medical agents such as social workers. (See Box 5.)

Confidentiality is not an absolute principle, and there are circumstances where it is permissible to disclose a patient's medical records to a third party.

Disclosure with patient consent

The first and most obvious exception is disclosure 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.

Disclosure without patient consent

Information can be disclosed without a patient's consent in two instances – if the disclosure is required by law or if the disclosure is in the public interest. This is the case whether the patient has explicitly refused consent or is incapable of giving consent.

Solicitors

Solicitors often ask for medical information. If the solicitor is acting for the patient, then before disclosing confidential information MPS recommends that a valid signed and dated mandate is provided.

Members of the clinical team

Patient care is usually team based and access to patient information is crucial for patient safety and continuity of care. 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 only exception is if withholding information from staff would place others at risk of death or serious harm.

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.

See paras 30.1 and 30.2 of the Medical Council's *Guide to Professional Conduct and Ethics for Registered Medical Practitioners*.

Court orders

Doctors should comply with a court or tribunal's order to disclose health records. Even if they have concerns about disclosing the records, they should still comply with the order and attach a covering letter to the judge describing their 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.

Box 6: Exceptions to the rule of confidentiality

"In certain limited circumstances, disclosure of patient information may be required by law. These circumstances are not limited to but may include:

- when ordered by a judge in a court of law, or by a tribunal or body established by an Act of the Oireachtas, or
- where mandated by infectious disease regulations.

In these instances, you should inform patients of the disclosure and the reasons for it."

Medical Council, *Guide to Professional Conduct and Ethics for Registered Medical Practitioners*, para 27.1

Case 4

Following a middle-aged man's sudden death, his insurance company sought information from his GP, relying on a declaration giving authority during the patient's lifetime for his medical details to be divulged. The GP was not satisfied with this, and asked the insurance company to obtain consent from the executors to the estate.

The insurance company renewed its request, this time with consent from the executors, but the GP felt undecided about how much information to include in her report. The medical record contained information about the patient's childhood experiences of sexual abuse, and she was sure that he would not have wanted even a mention of these painful memories to be exposed to strangers.

After talking it over with a medicolegal adviser at MPS, she decided that her first duty was to respect the confidentiality of the deceased and, as this particular aspect of his medical record had no bearing on the nature of the patient's death, she omitted it from her report to the insurance company.

Child protection

In any case involving the welfare of a child, the child's best interests are paramount. This may require disclosure of some content of the medical record – or details from it – to a social worker and/or the gardai. As a matter of good practice, you should always explain to the parents that you have a duty to refer your concerns to non-medical professionals and, where possible, obtain their consent to disclosure, except in rare circumstances, where to do so would put the child at increased risk.

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, reports to the cancer registry, etc – 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, with the best interests of the patient as a prime consideration in all decision making. It is essential that the reasons behind any decision to provide a third party with access to a patient's records be comprehensively documented.

See paras 6 and 7 of the Medical Council's *Guide to Professional Conduct and Ethics for Registered Medical Practitioners*.

Relatives

The only relatives who have a right to request access to a patient's records are those with parental responsibility for a minor under the age of 18. If, however, the minor concerned is sufficiently mature to understand the implications, his or her consent should be obtained before allowing access.

If the patient lacks capacity to consent to disclosure of his or her medical records, and those records are held by a public body, a family member may apply for access under the Freedom of Information Act. Records held by a private organisation should only be disclosed if the holder of the records is satisfied that it would be in the patient's interests to do so – to a solicitor, for example, where the patient's family is pursuing a personal injury claim on his or her behalf – or to comply with a court order.

If a patient has died, the rule of confidentiality still stands, but if the records relate to publicly funded care, certain categories of people, including next of kin, can apply for access to the medical records under the Freedom of Information Act. If the medical records are held by a private organisation, the medical records should only be disclosed with the consent of the next of kin or the executors of the deceased's estate (see Box 7).

See paras 26.1 and 26.2 of the Medical Council's *Guide to Professional Conduct and Ethics for Registered Medical Practitioners*.

Box 7: Next of kin

According to the Succession Act 1965, a person's next of kin is determined in the following order:

- Spouse
- Child or children
- Parents or surviving parent
- Brothers and sisters
- Nephews and nieces.

The gardai

In general, the gardai 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.
- In compliance with a court order.
- The public interest in disclosing information outweighs the public interest in preserving patient confidentiality.

Public interest justification to breach confidentiality

The public interest justification for disclosure usually turns on the threat of serious harm to others. Section 8 of the Data Protection Act lists a number of exceptions to the rules applying to data processing. This includes information held in a personal record that is "required for the purpose of preventing, detecting or investigating offences or prosecuting offenders" or "to prevent injury or other damage to the health of a person or serious loss of or damage to property".

The legislation does not elaborate on the seriousness of the offences or threats concerned, however. For doctors – who have a professional duty to protect the confidentiality of their patients – it would not be ethical to comply with any request for disclosure of sensitive personal information unless withholding the information would potentially have profound adverse consequences. Guidance published by the Information Commissioner might be of assistance here (see Box 8); it sets out the considerations that public bodies should take into account when deciding whether to withhold or disclose sensitive medical information under the Freedom of Information Act.

Box 8: Sensitive medical information

"Particular procedures must be followed in respect of medical information where the head of the body is of the opinion that its disclosure to the person concerned may be prejudicial to his or her health or emotional well-being. In these circumstances, if requested to do so by the person concerned, the public body shall instead release the record to an appropriate health professional nominated by the requester.

"The head has discretion to consider release of personal information to a third party only in exceptional circumstances where, on balance, he or she is of the opinion that the public interest in disclosure outweighs the right to privacy of the individual concerned, or where release of the information would benefit the individual."

Information Commissioner, *Short Guide to the FOI Acts*, p. 21

Publishing case reports, photographs and recordings

The patient's consent is also required before individual case histories, photographs or recordings can be published in media that the public has access to, even if they have been anonymised.

The Medical Council also recommends obtaining patients' express consent before using their case histories or photographs for education and training. (See Box 9.)

Box 9: Taking visual images for teaching

"Audio, visual or photographic recordings of a patient, or a relative of a patient, in which that person is identifiable should only be undertaken with their express consent. These recordings should be kept confidential as part of the patient's record."

Medical Council, *Guide to Professional Conduct and Ethics for Registered Medical Practitioners*, para 32.1

Security

When it comes to protecting privacy, medical records are the public's top concern, according to a survey commissioned by the Data Protection Commission in 2008.[1] This is hardly surprising considering the recent spate of high-profile cases, both in Ireland and the UK, in which sensitive patient information has either gone astray or been found in rubbish dumps.

The key to safeguarding your patients' confidential information is a sensible records management policy, incorporating strong security controls with clear policies governing access to and use of information contained in the records. There should also be policies setting out the circumstances in which certain information may and may not be disclosed and protocols for dealing with requests for access (see Appendix 2 for guidance on DPA and FOI requirements regarding access requests). The records management policy should apply to both computerised and manual records and include measures to protect the physical integrity of the records (See Appendix 1).

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. According to an article on records management in Ireland, "the average organisation … spends €120 in labour searching for a lost/misfiled document, loses 1 out of every 20 documents and office workers can each spend 400 hours per year looking for lost files. As between 1% & 5% of all documents are misfiled this is not really surprising."[2]

While the article's author bemoans the monetary cost to businesses, the implications for healthcare services are even more profound – many patient safety incidents have been attributed to lost and misplaced files, reports placed in the wrong records, mix-ups with patients' names and poor flagging up of crucial information such as drug allergies.

For the sake of efficiency and patient safety, every practice 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 15489:2001 – Information and Documentation: Records Management – can be purchased via the NSAI website.

There is also a European standard for electronic records management – MoReq2 – which has the advantage of being available as a free download (see Further reading for the link). This sets out the minimum software requirements for electronic records management – a useful tool for drawing up specifications for computerising a practice.

Retention of medical records

Retention periods

Until the Health Information Bill is passed into law, there are no national guidelines for the retention of healthcare records other than those produced by the National Hospitals Office for public hospitals. These, however, are based on common-sense principles that are equally applicable in the private sector (see Further reading on page 35 for the link to this document). In the absence of a national policy, MPS recommends the minimum retention periods set out in Box 10.

Box 10: Recommended minimum retention periods

- **Healthcare records of an adult** – eight years after last treatment or death.
- **Children and young people** – until the patient's 25th birthday, or 26th if the young person was 17 at the conclusion of treatment, or eight years after the patient's death. Guidelines for public hospitals also recommend keeping records for longer periods if the contents have relevance to adult conditions or have genetic implications.
- **Maternity records** – 25 years after the birth of the last child.
- **Records of a mentally disordered patient** – 20 years after last treatment or eight years after death.

The value of retaining records for longer periods is so they can assist in responding to a complaint or claim. The recommended minimum retention periods are guidelines only and it may sometimes be necessary to take an individual approach to some records and retain for longer periods.

Disposal of records

Clinical records may be transferred to the National Archives rather than be destroyed, if they are of archival value.

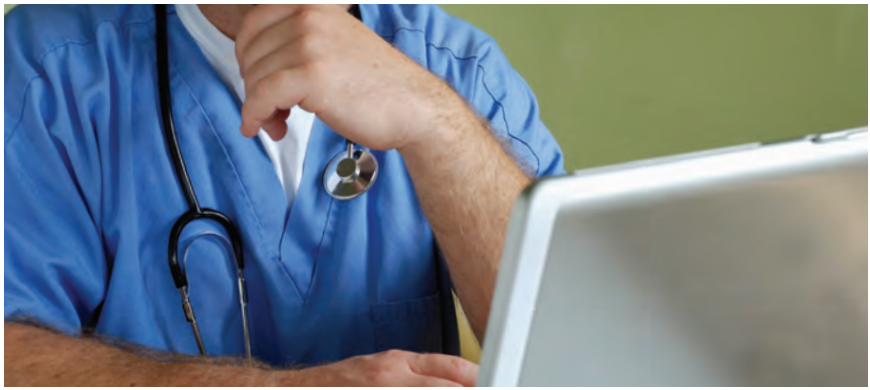
If records are to be destroyed, paper records should be shredded or incinerated. CDs, DVDs, hard disks and other forms of electronic storage should be overwritten with random data or physically destroyed. Be wary of selling or donating second-hand computers – "deleted" information can often still be 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 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.

Transferring records

If a patient transfers to another doctor, you should 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.



Research

If you are conducting your own research or audit based on your patients' medical records, it is acceptable to do so without the patient's consent, although as a matter of courtesy you should inform the patients concerned if it is feasible.

For studies involving outside researchers, any patient information you provide should be anonymised. If it is necessary to include information that could be used to identify individual patients, you must first secure the patient's express consent. The only exception to this is the submission of patient information to the National Cancer Registry Board, which is permissible by law.

Box 11: Educational research

"Education and training of health professionals is essential to the provision of safe and effective healthcare. When patient infor mation is to be used for education and training purposes, you should anonymise it as far as possible.

Where anonymisation is not possible or appropriate, you should make patients aware that their identifiable information may be disclosed for such purposes. They should have the opportunity to object to disclosure of their information and any such objection must be respected."

Medical Council, *Guide to Professional Conduct and Ethics for Registered Medical Practitioners*, para 30.3

Summary

- Keeping good clinical records is essential for continuity of care, especially when many clinicians are involved in delivering care. Good record keeping is an integral part of good medical practice.
- Records should include sufficient detail for someone else to take over a patient's care, seamlessly, from where you left off.
- Records that secure continuity of care will also be adequate for evidential purposes,in the event of a complaint, claim or disciplinary action.
- Clinical records should be clear, objective, contemporaneous, tamper-proof and original.
- Abbreviations, if used, must be unambiguous and universally understood.
- Clinical 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.
- Clinical records are sensitive personal data and must be kept securely to prevent damage and unauthorised access.
- Clinical records can usually be shared with other members of the clinical teams 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.
- All healthcare organisations holding clinical records must be registered (under the Data Protection Act) with the Information Commissioner.
- Where information from clinical records is required for audit and research purposes, anonymised data should be used wherever possible.
- Records should not be kept indefinitely but should be retained as long as they are relevant to patient care and associated legal and administrative purposes.
- Any alteration to written medical records should be immediately apparent to avoid any accusation that there has been an attempt to mislead or deceive.
- Similarly, with electronic records, any entries should be made clear to identify any changes.
- Common problems are illegibility of handwritten notes, failing to date and sign them, inaccurate recording of information and insufficient detail.

References

1. Data Protection Commissioner, Results of Data Protection Public Awareness Survey Published, Press Release (12 August 2008)

2. Andy Ellwood, Setting the Records Straight, Knowledge Ireland, April: 28–31 (2005)

Appendix 1: Environmental risks

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. Below are some of the factors that should be considered in a risk assessment.

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 – it is better to use professional offsite 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.

The risk of unauthorised access

Paper records should be kept in a room that can be securely locked when the practice is unattended. Limit the number of keys in circulation and keep a record of all key holders. If you use an electronic lock, only give the access code to staff who need it and change the code periodically.

Your records management policy and procedures should include protocols specifying the different roles of staff regarding access to records. Staff should be suitably trained so that they understand the legal and ethical principles of confidentiality and are aware of the need to keep records secure from unauthorised access.

Suitable safeguards for electronic records include firewalls, antivirus software, strong passwords, careful positioning of monitors so that information cannot be read by unauthorised people and setting access permissions on a need-to-know basis.

For basic and easily understandable guidance on safeguarding electronic medical records, you can't do better than to read *No Data No Business*, published by the General Practice Information Technology group of the Irish College of General Practitioners (see the Further reading section on page 35 for details).

For more comprehensive guidance on all aspects of records security, the ISO standard ISO27799 – Health Informatics: Information Security Management in Health Using ISO/IEC 27002 – covers everything you need to know (and more) about averting threats to the confidentiality, integrity and availability of your records. As the title suggests, this standard is based on ISO/IEC27002 – Code of Practice for Information Security Management – which essentially 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.

The standard can be purchased via the National Standards Authority of Ireland (NSAI) (see Further reading section on page 35 for links).

Appendix 2: Legal considerations

Data Protection Act 1988 and Data Protection (Amendment) Act 2003

The Data Protection Acts (DPA) place a number of responsibilities on individuals and organisations who hold data on identifiable living individuals, and corresponding rights to data subjects (in the clinical context, patients are data subjects). The Acts and their supporting regulations form a complex legal framework designed to protect people's privacy by preventing unauthorised or inappropriate use of their personal details.

Putting the Acts into practice boils down to complying with the eight data protection principles, which are relatively straightforward (see Box 12).

It is up to everybody working in an organisation that holds records containing personal information to comply with the spirit of the DPA – ie, respect the subject's privacy, keep the use of information to the minimum necessary and allow appropriate access.

Box 12: Data Protection Act

Data controllers must:

1. Obtain and process the information fairly
2. Keep it only for one or more specified and lawful purposes
3. Process it only in ways compatible with the purposes for which it was initially given
4. Keep it safe and secure
5. Keep it accurate and up-to-date
6. Ensure that it is adequate, relevant and not excessive
7. Retain it no longer than is necessary for the specified purpose or purposes
8. Give a copy of his/her personal data to any individual, on request.

Furthermore, personal information should not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. (This does not apply if the patient has consented to information being sent overseas.)

Private practice

If you are in private practice, you are required to register as a data controller and to demonstrate that you have an appropriate data protection policy in place. This applies both for records held in your private place of work and for any private practice you may have within a public hospital. A designated member of staff will need to take on the further responsibility of ensuring that the practice as a whole is complying with the Acts. You can be reasonably sure that you are working within DPA requirements as long as you:

- have registered as a data controller
- hold no more information about patients than is needed for their medical care, and you use it only for that purpose (though see Box 6 on page 14)
- institute robust security measures and confine access to authorised personnel on a need to know basis
- comply with patients' legitimate requests for access.

Requests for access

Under the terms of the DPA, patients have a right to access their own records, for which you may charge a small fee (no more than €6.35). You must comply with the request within 40 days. Before granting access, however, it is important to check the records to ensure that they do not include identifiable information about third parties, which should be edited out of any copy you make available to the patient. This does not generally include omitting letters or opinions contributed by colleagues, such as a letter from a consultant (see Box 13).

Box 13: Opinions expressed in the record

"Where personal data consists of an expression of opinion about the data subject by another person, the data subject has a right to access that opinion except if that opinion was given in confidence. If the opinion was not given in confidence then the possible identification of the individual who gave it does not exempt it from access."

Data Protection Commissioner, **www.dataprotection.ie**

There is no lower age limit specified by DPA legislation regarding access to one's own records. The Data Protection Commissioner has, however, endorsed the view taken by the Irish College of General Practice that 16-year-olds should be given access on request, and children below that age should be given access if the doctor is satisfied that they are mature enough to understand the implications.

Those with parental responsibility for a child can also request access to that child's records, but the confidentiality of mature minors should be respected, if it is likely that they might object to their records being disclosed.

Requests for access to the records of a patient who is mentally incapacitated must be decided on a case-by-case basis, bearing in mind that the interests of the patient are paramount.

You are permitted to withhold access to part or all of the record if there is a real possibility that viewing it would result in serious damage to the patient's physical, mental or emotional wellbeing. This would be a rare circumstance and such a decision should be based on sound clinical judgment. Your reasons for withholding the information should be clearly documented and you should indicate to the person requesting the record where omissions have been made. The patient has the right to ask the Data Protection Commissioner to investigate the matter, so it is important that your reasons for denying access are defensible.

Correcting the records

Data protection law gives individuals the right to request that inaccurate or misleading information be rectified. Such a request must be made in writing and you have 40 days in which to respond – either by making the amendment as requested or by giving reasons why you are not complying with the request.

This sort of situation is rarely straightforward – you might need to investigate the matter to confirm that the information in question is indeed inaccurate or misleading, and in most cases the best course is to arrange to meet the patient and discuss the issue.

If the information proves to be inaccurate, it should be erased or corrected, with a note saying that it was deleted at the request of the patient. If you find that the information is accurate, you should explain to the patient why it is important that it be retained in the record and offer to append a note detailing the patient's views.

You are under no obligation to erase or amend clinical information that has been fairly collected, relevant and accurate, and is not excessive for the purpose for which it was obtained. However, this raises the issues of confidentiality and consent; patients have the right to expect healthcare professionals to respect their wishes regarding disclosure of personal information. If the patient does not want certain information to be available to the healthcare team, you should agree to restrict access to it, but explain that this could compromise the patient's care.

Freedom of Information (FOI) Act

Patients – and in some instances relatives and others – can apply, under the FOI, for access to records held by publicly funded healthcare agencies. This also applies to medical card holders' GP records.

Case 5

A 56-year-old man had accessed his clinical records when dealing with a claim following a road traffic accident. While viewing them, he saw references to treatment for an STD some 12 years earlier and asked that they be erased.

His GP discussed the matter with him, ascertaining that the patient was worried that this information would "get out" and affect his reputation locally. The doctor assured him that the practice had strong measures in place to protect patients' confidentiality, but this did not put the patient's mind at rest. When the doctor offered to categorise this information as highly sensitive so that access would be restricted to himself, the patient was satisfied with this compromise.

As the STD had been successfully treated with no recurrence, the doctor felt that keeping the healthcare team in ignorance about this aspect of the patient's medical history was unlikely to have an adverse effect on his future care.

Appendix 3: NHO Standards for Content of the healthcare record

The following standards are only an extract from Part 2 of the NHO's *Code of Practice for Healthcare Records Management* (2007) available at www.lenus.ie. We recommend reading the full document.

Standard 7

The content of the healthcare record shall provide an accurate chronology of events and all significant consultations, assessments, observations, decisions, interventions and outcomes. The content of each record shall comply with clinical guidance provided by professional bodies and legal guidance provided by the Clinical Indemnity Scheme.

This standard shall apply to both hard copy and electronic documentation.

Rationale

The healthcare record and its content form an essential part of care allowing communication between healthcare professionals and demonstrating that the practitioner's duty of care has been fulfilled.

Correct identification

6. The patient's name shall be on each side of each page where patient information is documented and each page shall have the correct unique patient identification number and/or label. This shall also apply to every screen on computerised systems.

7. There shall be no blank spaces or pages between entries.

8. Before the healthcare professional makes an entry in the patient's healthcare record, s/he shall establish that the record belongs to the patient being attended. This shall be done by verifying with the patient and by cross-referencing the patient's wrist band with the healthcare record.

Legibility

9. All documentation shall be clear and legible.

10. When prescribing, writing shall be in un-joined lower case text or block capitals.

11. All entries shall be dated, timed and signed with a clear signature, printed name, title and bleep number (where relevant).

12. All entries shall be in permanent black ink.

Documenting date and time

13. It shall always be clear from the patient record the time that an event occurred and the time that a record was made.

14. The time (24-hour clock) and date (day/month/year) shall be noted against each clinical entry.

15. All entries shall be accurate in relation to date (day/month/year) and time.

Author identification

16. Each hospital site shall have an up-to-date signature bank of all clinical staff and non-clinical staff that may have occasion to write in the healthcare record.

17. Identification stamp pens, which have the clinician's name printed on a stamp attached to the pen, shall be permissible.

18. All signatures shall be accompanied by a printed name.

24. Records shall provide information on physical, psychological and social factors that may affect the patient.

25. The chronology of events and reasons for any decision made shall be recorded in the context of a thorough assessment of the patient including relevant history taking.

26. Records shall provide accurate, correct, comprehensive and concise information concerning the condition and care of the patient or client and associated observations.

27. Information shall be factual.

28. All entries in the record by healthcare professionals shall be made as soon as possible after each intervention and at least once every 24 hours during the working week for acute inpatient episodes. There shall be an entry in the record at least twice a week for rehabilitative care.

29. Every record entry (clinician related) shall identify the most senior clinician present at the time the entry was made.

30. The name of the primary clinician who is assuming overall responsibility for the patient's care shall be clearly identifiable in the healthcare record at all times. The name in the patient's record shall be the same clinician's name entered into the Patient Administration System (PAS). Should the primary clinician change during the course of treatment, this shall be noted on the healthcare record and on the PAS.

31. Input into all records shall be multidisciplinary.

Retrospective entries

32. Retrospective documentation shall be:
    - Dated.
    - Timed.
    - Signed (and counter-signed as appropriate).

33. The reason why the retrospective entry is being made shall be clearly stated.

34. It shall be clear that the entry is a retrospective entry.

Relevancy

40. Records shall be objective and shall describe what is observed.

41. If an incident has not been observed but is relevant to client care then this shall be clear, eg, patient states that...

Verbal instructions

42. Instructions regarding patient care from a healthcare professional via the telephone shall be documented, dated, signed and counter-signed by the healthcare professional responsible for giving the instructions.

43. If no instructions were given, this shall also be documented.

Abnormal results

44. There shall be a note in the clinical record of any significant abnormal results found or communicated to the healthcare professional. This shall include a record of who has been informed, eg, healthcare professional's name. This note shall be made by the appropriate healthcare professional.

Medications

45. Drugs shall only be administered and documented in the presence of clear unambiguous prescriptions and in accordance with hospital policies.

46. Drug names shall never be abbreviated under any circumstances.

47. Generic names ONLY shall be used for the drug chart.

48. The choice of therapeutic agents used shall remain the responsibility of the clinician.

Language

49. Records shall be written in English.

50. Records shall be completed in terms that the patient and/or the healthcare professional can understand.

51. Records shall be supported by explanations where this may not be possible.

52. Records shall be phrased clearly and unambiguously.

53. Records shall be objective, factual, devoid of jargon, witticisms or derogatory remarks.

Advice

54. Healthcare professionals advice on care, in any format (eg, verbal, leaflet), shall be documented in notes of advice given.

Patient alerts and allergies

56. Alerts and allergies shall be recorded on the inside of the cover of the healthcare record chart.

57. The information shall be signed and dated and there is an end date for the alert, if appropriate.

58. The hospital shall have a clear procedure regarding who should enter alerts into the healthcare record, when alerts should be entered and the procedure for removing alerts from the healthcare record. These procedures shall be adhered to.

Admission entry

65. The following minimum, general patient information shall be included in the record entry for acute medical admissions and may also be supplemented with additional specialty information:
    - Reason for clinical encounter.
    - Presenting problem/complaint.
    - History of presenting problem.
    - Current diagnoses.
    - Patient Alerts/Allergies (this should also be recorded on the inside of the front cover).
    - Past illnesses.
    - Procedures and investigations.
    - Medications and diets including nutritional supplements.
    - Social circumstances.
    - Functional state (Self-care/baseline mobility/walking aids and appliances).
    - Family history.
    - Systems review.
    - Examination findings.
    - Results of investigations.
    - Problem list.
    - Overall assessment.
    - Management plan.
    - Intended outcomes.
    - Information given to patient.

Follow-up entry

66. The following patient information shall be included in the follow-up entries for acute medical admissions:

- Reason for clinical encounter.
- Review of case.
- Overall assessment including any change
- since previous encounter.
- Management care plan.
- Information given to patient and carers.

Documenting consent in the healthcare record

72. Consent shall:

- Be easily and clearly identifiable either on a consent form, which is retained as part of the clinical record, or in the case of verbal consent, documented within the clinical record.
- Contain no abbreviations.
- Clearly state the procedure/treatment/care involved and the risks and benefits of that procedure.
- Clearly identify the patient by name and healthcare record number.
- Clearly identify who has granted or refused consent and/or their relationship to the patient in the case of parent/guardian.
- Have a documented record of what appropriate patient/client information or relevant discussions have been provided to the patient/guardian detailing the procedure/treatment/care, risks, benefits and/or alternative.
- Have a documented record of how this information has been provided (eg, patient/client information leaflets, verbally, etc).
- Be dated and signed by the healthcare professional obtaining the consent, including full name and grade.

73. Verbal consent shall be documented in the clinical record and shall clearly identify the witness, eg, by name and grade.

74. This standard shall apply to both hard copy and electronic documentation.

Further reading

Data Protection Commissioner's website **www.dataprotection.ie**

General Practice Information Technology (GPIT) Group, *No Data No Business* (2008) **www.icgp.ie/go/in_the_practice/information_technology/publications_reports.** This webpage also contains pdfs of other useful guidance and reports.

Information Commissioner's website **www.oic.gov.ie**

Model Requirements Specification for the Management of Electronic Records (MoReq2) **www.moreq2.eu**. The specifications can be downloaded free from this site.

National Hospitals Office, *Code of Practice for Healthcare Records Management* (2007). The full document can be downloaded from **www.lenus.ie**

Medical Council, *Guide to Professional Conduct and Ethics for Registered Medical Practitioners*, paras 23.1 and 23.2

National Standards Authority of Ireland **www.nsai.ie**. This site links to an online catalogue of international standards at **www.standards.ie** where you can purchase ISO15489:2001 (Information and Documentation – Records Management), ISO27799 (Health Informatics: Information Security Management in Health Using ISO/IEC27002) and ISO/IEC27001 (Information Technology Security Techniques/Information Security Management Systems Requirements).

MEDICAL PROTECTION SOCIETY
PROFESSIONAL SUPPORT AND EXPERT ADVICE

MPS Putting members **first**

www.medicalprotection.org/ireland

General enquiries
T +44 (0) 113 243 6436
F +44 (0) 113 243 0500
E info@mps.org.uk

Medicolegal enquiries
T +44 (0) 113 243 6436
F +44 (0) 113 243 0500
E querydoc@mps.org.uk

Membership enquiries
T 1800 509 441
F +44 (0) 113 243 0500
E member.help@mps.org.uk

Calls to Membership Services may be recorded for monitoring and training purposes.

Please direct all comments, questions or suggestions about MPS service, policy and operations to:

Chief Executive
Medical Protection Society
33 Cavendish Square,
London W1G 0PS, United Kingdom

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

MPS0901: 09/13