Royal College of Nursing

# Confidentiality

*RCN guidance for occupational health nurses*

Royal College of Nursing


## Acknowledgements

Carol Bannister
RCN Occupational Health Nursing Adviser

Chris Cox
RCN Assistant Director of Legal Services

Sharon Horan
Chair, RCN Society of Occupational Health Nursing

Jan Maw
RCN Society of Occupational Health Nursing

## Critical readers

**Members of the RCN Society of Occupational Health Nursing Steering Committee**

Sheelagh Brewer
RCN Senior Employment Relations Officer

Nola Ishmael
Department of Health (England) Nursing Officer

Bernie Jackson
Chair RCN Occupational Health Managers Forum

Nicola Lee
RCN Work Injured Nurses Group Adviser


## Abbreviations

| | |
|---|---|
| BMA | British Medical Association |
| DDA | Disability Discrimination Act |
| DPA | Data Protection Act |
| FOM | Faculty of Occupational Medicine |
| GMC | General Medical Council |
| NMC | Nursing and Midwifery Council |
| OH | Occupational health |
| OHN | Occupational health nurses |
| RCN | Royal College of Nursing |
| UKCC | United Kingdom Council for Nursing, Midwifery and Health Visiting |

## Case studies

1 *W* v *Egdell* (1990) 1 All ER 835

2 *X* v *Y* (1988) 2 All ER 649

3 *London Borough of Hammersmith & Fulham* v *Farnsworth* (2000) IRLR 691

4 *Dunn* v *British Coal Corporation* (1993) ICR 59

## Scenarios

1 Peer pressure

2 Pre-employment data

3 Breaking the boundaries

4 Public interest

5 Withholding consent

6 Employer pressure

Published by the Royal College of Nursing, 20 Cavendish Square, London, W1G 0RN

# Confidentiality:

## *RCN guidance for occupational health nurses*

## Contents

# 1 Introduction

To ensure the effective use of an occupational health service that contributes to a healthy workplace and workforce, occupational health practitioners need to work collaboratively with both employers and workers. A clear and shared understanding of the legal and professional obligations of both practitioner and employer, together with the sensitive handling of confidential information, are keys to achieving this.

If an employee believes that medical confidences will not be respected, the relationship between health professional, employer and patient or client suffers and cannot function effectively.

The professional ethical obligations for nurses are set out in the Nursing and Midwifery Council's (NMC) new *Code of professional practice* published in April 2002. It combines the existing *Scope of professional practice, Guidelines for professional practice* and the *Code of professional practice,* published by the former regulatory body the United Kingdom Council for Nursing Midwifery and Health Visiting (UKCC).

"To trust another person with private and personal information about yourself is a significant matter. If the person to whom that information is given is a nurse, midwife or health visitor, the patient or client has a right to believe that this information, given in confidence, will only be used for the purposes for which it was given and will not be released to others without their permission. The death of a patient or client does not give you the right to break confidentiality."

NMC, 2002

The code of professional practice for doctors is described in *Duties of a doctor* (GMC, 1995), and *Confidentiality: protecting and providing information* (GMC, 2000).

Health professionals, whether working in the NHS or private sector, should also observe any Government guidelines on confidentiality such as the Department of Health *Code of Practice on Confidentiality* (2003).

This guidance looks at the particular challenges faced by occupational health professionals in dealing with confidential information, and the potential for conflict of interest and loyalty. It will guide you through:

- what the law says
- what your legal, professional and ethical responsibilities are.

2

# The law and you

If confidentiality is broken an individual can sue through a civil court. That person can also complain to the Information Commissioner if there is a breach of the 1998 Data Protection Act (DPA). The right to confidentiality is protected by:

- common law
- Article 8 of the European Convention on Human Rights now incorporated in UK law by the Human Rights Act 1998
- Data Protection Act 1998.

Lord Goff in the famous Spycatcher case (*Attorney General* v *Guardian Newspapers Ltd* No 2 [1990] 1 AC 109) summarised the duty of confidence as follows:

"A duty of confidence arises when confidential information comes to the knowledge of a person (the confidant) in circumstances where he has notice, or is held to have agreed, that the information is confidential, with the effect that it would be just in all the circumstances that he should be precluded from disclosing the information to others."

## Human Rights Act 1998

The Human Rights Act 1998 came into force in October 2000. The impact of the Act on how health care is practiced in the UK has been limited to date. The British Medical Association (BMA) advises its members that:

"the requirements of the Human Rights Act reflect, very closely, existing good practice. Decisions taken by doctors on the basis of current ethical standards are likely to be compliant with the Act".

A breach of confidentiality is likely to breach the UK's obligation under Article 8(1) of the European Convention (Schedule 1 of the 1998 Act), which guarantees the right to respect for private life. In *Z* v *Finland* (1998) 25 EHRR 371, the European Court commented:

"The protection of personal data, not least medical data, is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the Convention. Respecting confidentiality of health data is a vital principle in the legal systems of all the contracting parties to the Convention. It is crucial not only to respect the privacy of the patient but also to preserve his or her confidence in the medical profession and in the health services in general."

Article 8 is not an absolute right, so Article 8(2) allows for certain exceptions where the state may interfere with an individual's right to privacy. This may be for the prevention of crime and disorder, where there is a need to protect the health, or the rights and freedoms of others. Nevertheless, any interference must be in accordance with the law, and proportionate with the aim being pursued, by limiting the human right in question.

NHS trusts are public authorities and are therefore covered by the European Convention. This relates to the trust's public (e.g. health care) and private (e.g. employment) activities. The position of private sector bodies is more complex, but it should be assumed that the keeping of health records by health care professionals is covered by the Convention, whether in the private or public sectors.

## Data Protection Act 1998

The Data Protection Act 1988 came into effect in October 2001. It relates to both computerised, or electronic, and manual records. It supersedes the Access to Health Records Act 1990.

The Act strengthens the controls around the processing (collection, storage, use and disclosure) of data. Importantly, the Act applies not just to data that is processed automatically, but extends to paper-based records held in relevant filing systems which includes occupational health records.

Registered health care practitioners must make sure that, where possible, the storage and movement of records in health care settings does not put the confidentiality of patient/client information at risk. (NMC, 2000)

An individual who suffers damage because of any contravention of the Act has a right to compensation. The eight data protection principles state that personal data must be:

1 fairly and lawfully processed

2 processed for limited purposes and not in any manner incompatible with those purposes

3 adequate, relevant and not excessive

4 accurate

5 not kept for longer than necessary

6 processed in accordance with individuals' rights

7 secure

8 not transferred to countries without adequate protection.

The Act introduces several new definitions that are important for you to understand, including:

- personal data: data that relates to a living individual who can be identified from those data or from those data and other information which is in the possession of, or likely to come into the possession of, the data controller
- data subject: an individual who is the subject of the personal data
- data controller: a person who (either alone or jointly or in common with other persons) determines the purposes for which, and the manner in which, any personal data is, or is to be, processed
- data processor: people who obtain, record or hold the data or carry out any operation or set of operations on the data. It includes organising, adapting and amending the data, retrieval, consultation and use of the data, disclosure and erasure or destruction of the data
- on computer: the term computer includes any type of computer however described, such as mainframe, desktop, laptop, palmtop and so on. It also includes other types of equipment that although not normally described as computers, nevertheless have some ability to process automatically. For example, automatic retrieval systems for microfilm and microfiche, audio and visual systems (including CCTV), electronic flexitime systems and telephone logging equipment
- sensitive data: includes information as to an individual's "physical or mental health or condition" and "sexual life".

People have a right to know why information is collected, and that data is only used for the stated purpose. They also have a right of access under the Act to personal data held on them and to have inaccuracies corrected, removed or destroyed. Appropriate technical and organisational measures must be taken against unauthorised or unlawful processing of personal information, and against its accidental loss or destruction, or damage. Personal data must be processed fairly and lawfully and, in the case of sensitive data only if certain conditions are met. Health professionals may process health records where:

- an individual has given explicit consent
- it is necessary for medical purposes
- it is necessary to exercise or perform any right or obligation that is conferred or imposed by law on the data controller in connection with employment
- it is necessary to protect the vital interest of the individual concerned or another person, provided that:
  - consent cannot be given by or on behalf of the individual concerned
  - the data controller cannot reasonably be expected to obtain the consent of the individual concerned
  - consent by or on behalf of the individual concerned has been unreasonably refused in the case of protection of the vital interests of another person.

The definition of medical purposes includes:

- preventive medicine
- medical diagnosis by a health professional or someone who owes a similar duty of confidentiality
- medical research
- the provision of care and treatment; management of health care services (this list is not exhaustive).

The Secretary of State has the power to make exemptions or modifications to the "subject information provisions" of the Act. This includes the rights of access to personal data. Under the Data Protection (Subject Access Modification) (Health) Order 2000, access may be denied. This is based on the extent to which it is likely to cause serious harm to the physical or mental health of the individual concerned or any other person, or would breach the confidences of third parties.

A data controller may not refuse access on the grounds that the identity of a third party would be disclosed, where the information is contained in a health record and the third party is a health professional who has:

- compiled or contributed to that health record
- been involved in the care of the data subject.

However, access may be refused if the health professional's physical or mental health is likely to suffer serious harm if access is given.

Under the 1998 Act the information in the health record must be communicated in a form which is capable of being understood. Occupational health nurses (OHN) and doctors should be prepared to interpret and explain the information in the record.

How occupational health (OH) practitioners use information gathered during pre and post-employment screening should be given serious consideration. Data can only be used for the purposes for which it was given. Therefore, it is likely that OH practitioners may be in breach of the Act if, for example, they use data collected on pre-employment selection questionnaires for post-employment monitoring or research. This is because it is unlikely that the individual has given consent to use such data for multiple purposes. Practitioners are advised to consult the website of the Information Commissioner, in particular, his *Employment Practices Data Protection Code: Part 4 Information About Worker's Health (OIC, 2005),* for up to date advice on the application of the Act to the processing of health data in an employment setting.

## Access to Medical Reports Act 1988

The Access to Medical Reports Act 1988 gives patients a right of access to reports prepared for insurance or employment purposes. The Act only applies to reports made after 1 January, 1989.

Anyone commissioning a report for insurance or employment purposes must obtain the consent of the patient who is the subject of the report. The latter has the right to see the report before it is sent to the employer or insurer. The patient/client may also veto its release and attach comments on any matters that they consider are inaccurate.

Even if the patient/client does not exercise their right to see the report in advance, the right of access remains for six months after its release.

However, a doctor is only obliged to divulge information under the Act if he is or has been responsible for the patient's clinical care. Therefore, while the Act clearly covers a GP's report, or treating consultant, it remains unclear whether a report commissioned from an independent doctor is covered. The definition of care in the Act is very wide. It includes examination, investigation or diagnosis for the purposes of, or in connection with, any form of medical treatment (section 2(1)).

For OH practitioners it has been argued that there is a legal duty to protect the health of all those in the workplace, even people who have never consulted the medical practitioner (*Stokes* v *Guest Keen* [1968] 1 WLR 1776). Accordingly, all consultations are potentially covered by the Act, and good practice suggests compliance in all cases.

However, under the Act doctors may refuse access to information if it could:

- cause serious harm to the physical or mental health of the individual who has asked for access, or to others
- identify another, unless that third party consents, or is another health professional involved in the care of the patient
- indicate the intentions of the practitioner in respect of the patient.

These exceptions can apply to all or part of the report, but the patient must be told whether access is being denied.

## Access to Health Records Act 1990

Access to manual health records made since 1 November 1991 was available under the Access to Health Records Act 1990. However, this Act lost much of its significance with the implementation of the Data Protection Act 1998, and remains relevant only in relation to deceased patients.

## The Computer Misuse Act 1990

The Act came into force to secure computer programs and data against unauthorised access or alteration. Authorised users have permission to use certain programmes and data. It is a criminal offence if those users go beyond what is permitted. The Act makes provision for accidentally exceeding permission and covers fraud, extortion and blackmail.

The same basic principles that apply to manual records apply to computer-held records. OH professionals are accountable for making sure that whatever system is used is fully secure. It must have robust local protocols in place that specify which staff have access to computer-held records, and make clear access boundaries and responsibilities.

The NMC position statement on computer confidentiality is:

"In order to safeguard information which is stored on a computer system, it is important to know exactly who will have access to the information which a practitioner will be feeding into the system. Where it has become clear that access to information contained in a computer filing system is available to members of staff who are not registered practitioners, or health professionals governed by similar ethical principles, an important clause concerning confidentiality should appear within those persons' contracts of employment."

*NMC, 2002*

The key messages are that:

- you are accountable for any entry you make in electronic-held records
- you must ensure that any entry you make is clear
- the identity of the person who made the record is clearly indicated
- the methods you use for recording information are secure
- the categories of staff who have access to records are clearly identified
- procedures are in place to check whether a record is authentic when there is no written signature.

# 3 Ownership of confidential records

There is a clear distinction between ownership of records and control over the contents of those records.

Case law, in relation to NHS patients (see *R* v *Mid Glamorgan FHSA ex part Martin* [1995] 1 All ER 356), states that legal ownership of health records resides in the organisation (for example, hospital, PCT) owning the paper, IT and so on, on which the health information is stored. The same reasoning applies to OH records that are made on employer's paper and stored on their premises. This means that the employer generally owns OH records.

However, common law duty mirrors statutory duty under the DPA. Therefore, the law binds the owner of records on confidentiality. The content of a record generally remains the property of the person who made it, in most cases, the OH professional. Nevertheless, legal ownership does not give the owner an absolute right to deal with the record in any way it chooses. The duty of confidentiality, both at common law and under statute, binds the owner of the health record, giving ultimate control over its content to the record's subject, namely the employee.

Whoever is in possession of medical records owes a legal duty of care to the subject of those records. They must take reasonable care for their security and ensure that the contents are not made known to anyone without the authority to read them.

In circumstances where an OHN or doctor resigns from their post, records should be transferred to the control of the remaining, or newly appointed OHN or doctor. In cases where OHNs and/or doctors have been made redundant and the business closed, the RCN recommend that records are transferred with individual consent either to each employee's own doctor or to another medical adviser.

Destroying health records before the recommended archive time has elapsed is unacceptable practice. The original paper-based records can only be destroyed when data has been transferred or copied to electronic or microfilm storage (it is not necessary to transfer paper records to electronic or microfilm storage after the elapsed archive time, following which paper records can be destroyed). The Department of Health (DH) recommends retaining records for a minimum of eight years after the last entry, while the BMA recommends ten years. The DH consultation on records, *Management: NHS Code of Practice (2005)* suggests that a new minimum retention period for ocupational health records (staff) should be three years.

### Lines of action for transfer of medical records in summary

1. If there is a nurse or doctor, they can assume responsibility for the records.
2. Where there is no nurse or doctor, negotiate appropriate transfer arrangements with the employer, and where possible a trade union representative.
3. Where agreement is reached, transfer personal medical records to individuals or GPs.
4. Record the date that records are transferred and to whom.
5. If there is no agreement, negotiate for records to remain locked in secure place and keys to be held by a named persons such as a human resources or employee representative.
6. Write to the employer outlining any agreed arrangements, and remind them of their duty of confidentiality.

### Scenario one
Peer pressure

Dr Smith was employed for several years as the part-time occupational health physician for a large manufacturing company called ManComp. He left to take up another post in a different part of the country. Sometime after he had left, he was asked to give evidence at a tribunal concerning treatment provided to a ManComp employee. Dr Smith contacted the nurse at ManComp and asked for copies of the records to be sent to him so that he could refresh his memory before giving evidence. He told the nurse because he had written the records it would not be a breach of confidentiality.

**Facts**

- The doctor had no automatic right of access to the medical records of a patient/client who was no longer under his care.
- The nurse did not have the explicit consent of employee to release the information.

**Conclusions**

- The nurse should not send copies of the records without the explicit consent of the employee.
- The nurse should advise the doctor that if the medical notes are required for court proceedings, then he should ask the relevant lawyers to produce a copy of the court order requiring disclosure.

# 4 Access to confidential records

OHNs should not always assume that patients/clients have given implied consent for disclosure of confidential information to other members of the team, even on a need to know basis for the management of their care. Patients/clients must be aware of who will have access to their information and why, and have the right to withdraw consent to sharing the information.

Nurses frequently find themselves in challenging situations with regards to the confidential status of pre-employment screening forms, health surveillance data and occupational health records.

Clear policies and procedures should be in place which explicitly state:

- what data is to be collected
- who will be able to access it
- what the definitions of 'confidential' and 'confidentiality' are
- that 'confidential' data will not be released without the 'informed consent' of the person/s who are the subject of that data.

Health information is generally classed as both 'confidential' and 'sensitive personal' data according to the Data Protection Act 1998 and should only be processed accordingly. It is poor practice to seek pre-employment health information on forms that do not specify that the information is 'confidential' and restricted to the Occupational Health department.

Where clinical data needs to be shared with other members of the OH department, the doctor or nurse must ensure that those colleagues are aware of their personal responsibility to keep information confidential.

Employees, who access or handle confidential records, although they are not directly involved in patient care, must have contracts of employment that contain clauses emphasising the principles of confidentiality. They should also state what disciplinary action could result if these principles are not met.

If it is appropriate to share information gained from your work with other health or social work practitioners, you must be satisfied it will be kept in strict professional confidence, and used only for the purpose for which it was given.

Many student OHNs work as staff nurses in occupational health departments. This means that they are accountable under the NMC *Code of Professional Conduct* to protect confidential information. Where other students work in OH departments for practice experience, the OH manager is responsible for the security of patient/client records and for closely supervising access to the information.

It is important that you have explicit informed consent from the patient/client to share information with other health care professionals. You must ensure that the patient/client understands which information will be made available to other members of the team, what standards of confidentiality will be maintained.

### Scenario two
### Pre-employment data

You have recently joined a new company. The pre-employment screening form does not state that the information is confidential and restricted to the occupational health depatment. Having screened several forms, you advise Human Resources (HR) that all but one of the candidates is 'fit' and that one other is 'fit, with some adjustment to the work station'. Later that day, you are requested to send the pre-employment screening forms to the HR department. Should you do this?

**Answer**

Whilst this is poor practice, legally there is nothing to prevent HR from seeking access to this information, if the pre-employment form did not state that the information was confidential and restricted to the occupational health department. If the information was provided freely under these conditions, then confidentiality has not been breached. If a nurse refuses access to the information under these conditions then they could be open to disciplinary action by their employer.

**Action**

You should advise your employer that accessing pre-employment screening data is poor practice, because prospective employees are more likely to be honest about their medical history if the information remains confidential and restricted to the occupational health department. Furthermore, decisions about medical fitness should be made only by competent staff and, if managers or HR make an erroneous decision based on declared health conditions, the prospective employee

has grounds to take a grievance out against the company under, for example, the Disability Discrimination Act (DDA 1995, 2005).

You should clarify the role of the occupational health department in advising on 'fitness', 'fitness with reasonable adjustment' and 'non fitness'. Reassure your employer that 'informed consent' would be sought from a prospective employee should there be a need to discuss any medical condition that required discussion with the wider organisation, both to secure reasonable adjustment of facilities and to maintain the safety of the individual.

Finally, you should draw to the attention of HR that general access to confidential occupational health information breaches the Information Commissioner's *Employment Practices Data Protection Code, Part 4: Information about Worker's Health (2004)*. Additionally, both the Data Protection Act (1998) and the Information Commissioner's Code emphasises:

- the notions of 'explicit' and 'implicit' consent
- the general confidentiality of the occupational health information
- the need to use qualified occupational health personnel to assess fitness.

If the employer continues to insist on accessing pre-employment screening forms,you should make a record of the advice that you gave.

# 5 Disclosure of confidential information

Records containing personal information are protected against disclosure unless there is consent or some other overriding legal reason justifying disclosure. Therefore, you must always in the first instance try to obtain explicit consent of a patient/client before you disclose confidential information. You must make sure that the patient/client can make an informed response as to whether that information can be disclosed.

The Faculty of Occupational Medicine (FOM) *Guidance on Ethics for Occupational Physicians* (Faculty of Occupational Medicine 1999) document identifies seven situations where confidential information may be disclosed. They broadly compare with those described in the GMC guidance *Confidentiality, protecting and providing information*, published in September 2000, and the NMC *Code of Professional Conduct*. The seven situations are:

1. with the consent of the client
2. if disclosure is clearly in the patient's interest but it is not possible or is undesirable to seek consent
3. if it is required by law
4. if it is unequivocally in the public interest
5. if it is necessary to safeguard national security or to prevent a serious crime
6. if it will prevent a serious risk to public health
7. in certain circumstances for the purposes of medical research.

## Scenario three
### Breaking the boundaries

Nurse X had completed a post registration programme in paediatrics and had applied for a post on the children's unit. She had been a student nurse at the same hospital and the occupational health department (OHD) knew her past medical history. She had suffered several bouts of ill health during her student nurse training, and during her paediatric course was diagnosed with Crohns disease for which she was admitted for surgery.

She went on to complete her paediatric course successfully, and undertook her final placement on the children's unit. She completed and returned a pre-employment screening form that clearly stated that the information was confidential to the OHD.

Following pre-employment assessment, the OHD sent a letter to the unit manager recommending that the nurse X was not fit for the post. The letter gave details of the applicant's past medical history including sickness-absence attributable to bouts of diarrhoea. It concluded that nurse X was unfit for the post because of the risk of cross infection. The manager informed nurse X of the detail of the letter, because of the excellent standards of practice that nurse X had demonstrated while on placement at the unit, took the decision to disregard the recommendation of the OHD and employed her.

**Facts**

- This was a clear breach of confidentiality. At no time was consent sought or given for confidential medical details to be given to the unit manager.
- Had the manager followed the recommendations of the OHD the applicant may have had sufficient grounds to take out a civil action for loss of earnings and distress.
- The applicant does have sufficient grounds to take a grievance for professional misconduct to the GMC and/or the NMC.
- Where misconduct is found, the GMC or NMC have the authority to investigate, warn and/or suspend and/or remove a practitioner from their registers.

**Conclusions**

- Where pre-employment forms clearly state that information given is confidential to the OHD the information must be treated as such, unless there is explicit consent.
- Where information has to be discussed with third parties so that the employer can make reasonable adjustments under the Disability Discrimination Act, the applicant should be fully informed.
- Applicants have the right to know what information about them will be given and to whom.
- Managers have the right to disregard recommendations of the OHD, but good practice would include appropriate dialogue and consideration of the facts before doing so.
- Applicants have the right to pursue recompense for grievances through statutory and professional bodies.

6

# Disclosure in the public interest

All the health professional codes of practice recognise that in certain circumstances the public interest in disclosure outweighs the public interest in ensuring confidentiality.

Case studies one, two and three highlight the difficult ethical and legal dilemmas that health care professionals may face. Given the variety of situations that may give rise to such dilemmas each situation must be considered on its merits.

The GMC guidance says that:

"Disclosures may be necessary in the public interest where a failure to disclose information may expose the patient, or others, to risk of death or serious harm. In such circumstances you should disclose information promptly to an appropriate person or authority."

The NMC guidance says that:

"You are responsible for any decision that you make to release confidential information because you think that this is in the public's best interest; if you choose to break confidentiality because you believe that this is in the public's best interest, you must have considered the situation carefully enough to justify that decision."

If the person claiming confidentiality presents a threat to the public interest, they will not be entitled to rely on the protection of the law. An example of this, is highlighted in case study one *W* v *Egdell* [1990] 1 All ER 835. Three principles emerge from the case:

1 a real and serious risk of danger to the public must be shown for the exception to apply

2 disclosure must be to a person who has a legitimate interest to receive the information. For example, in Egdell the court indicated that it would have been a breach of confidence to have disclosed the information to the press

3 disclosure must be confined to that which is strictly necessary (not necessarily all of the details).

Conversely, case study two *X* v *Y* [1988] 2 All ER 649 provides an example of where the exercise of balancing the public interest led to a court order forbidding the disclosure of confidential information.

### Case study one
*W* v *Egdell* [1990] 1 All ER 835

W was detained as a patient in a secure hospital after he had killed five people and wounded two others. Following an application for a review by a Mental Health Review Tribunal for discharge, or transfer with a view to discharge, W's solicitors instructed Dr Egdell to produce a report supporting W's application.

Dr Egdell opposed the transfer, and because of his report, W, through his solicitors, withdrew his application. Dr Egdell remained concerned that neither the tribunal nor the secure hospital was aware of his report, and so sent a copy to the hospital's medical director. This was forwarded to the Secretary of State.

The Court of Appeal, hearing W's action for breach of the Dr Egdell's duty of confidence, found that the public interest justified disclosure to the medical director and the Home Office. Neither of these parties was aware of Dr Egdell's information about W's dangerousness, and it was in the public interest that the authorities responsible for protecting the public safety took their decisions based on the best available information.

Accordingly, the public interest in protecting the public took precedence over the general public interest in ensuring the confidentiality of medical records and reports.

### Case study two
*X* v *Y* [1988] 2 All ER 649

Employees of a health authority gave a newspaper the names of two practicing doctors who had AIDS. The judge concluded that the public interest in maintaining confidence in the circumstances of AIDS was a significant and fundamental one. The expert testimony that he accepted suggested that preventing the spread of the virus would be seriously impeded if people who might be infected could not disclose this fact to health professionals knowing that the information would remain confidential. The public interest in the freedom of the press was outweighed in this respect.

# 7 Serious risk to public health and prevention of serious crime

The clear principle running through all professional codes is that without consent, disclosure must only take place in exceptional circumstances.

The principles on the disclosure of confidential information in the public interest that we have outlined above could apply to situations where there could be a serious risk to public health, or disclosure could prevent serious crime.

For example, health care professionals infected with HIV or hepatitis who continue to work should refer to: the UKCC Registrar's letter and statement (dated 6 April 1993); the GMC's booklet *HIV and AIDS: the ethical considerations* (October 1995); the guidance of the Expert Advisory Group on AIDS (March 1994, revised December 1998) *AIDS/HIV – infected health care workers: guidance on the management of infected health care workers*; and *Hepatitis B infected health care workers* (2000/020) and *Hepatitis C infected health care workers* (2002/010) both available from www.dh.gov.uk.

Remember you will always be held accountable when you release information, whatever the circumstances including if you have been under pressure to do so. In all cases where you deliberately release information, even if you believe it to be in the best interests of the public, you must be able to justify your decision.

If you are unclear or uncertain making a decision to release information without consent, you should ask advice from other professional colleagues. If appropriate, you can also consult the NMC or RCN. If you decide to disclose information, you should record your reasons either in the appropriate record or in a special note that can be kept in a separate file. This is outlined in the NMC's booklet *Guidelines for records and record keeping*.

## Scenario four
### Public interest

Nurse White was leaving the factory when she saw an employee leaving the car park on a motor cycle. Three weeks previously the employee's diabetes had become unstable and he had suffered from several hypoglycaemic attacks and been hospitalised. The OHD had been involved in his rehabilitation, and he had been allowed to return to work while he was monitored for a new insulin regime. However, he had been told by his doctor and consultant that he must not drive until his condition was stable. He had been re-deployed from his job in the warehouse, which included fork lift truck driving, to general office duties pending clearance from the doctor and consultant.

**Facts**

- The nurse had discussed with management and personnel reasonable adjustments to the employee's work, and a review date had been agreed with the employee's consent.
- The nurse faced a moral dilemma because the employee was not putting himself or others at risk while at work.
- Both the nurse and the employee were aware that to drive before his diabetes was stabilised could put both himself and the public at risk.

**Conclusions**

- The NMC *Code of Professional Conduct* gives clear guidance on this issue. There are legitimate reasons to break confidentiality if not to do so might harm the patient or the public.
- Under the NMC *Code of Professional Conduct* the nurse should advise the employee of her concerns and her duties if possible before breaking a confidence.
- She could inform the employee that she is left with no alternative but to inform the GP. As the employee's medical care provider it is the GP's responsibility to inform the relevant authorities of any restrictions to driving due to medical conditions.
- The nurse must carefully record the advice and actions that are taken.

# 8 Whistleblowing

The 1998 Public Interest Disclosure Act came into effect on 2 July 1999. It reflects widespread belief that workers who have genuine concerns about apparent malpractice in the workplace need specific protection against victimisation if they are going to be encouraged to raise those concerns. It is hoped that the Act will promote good governance and openness in organisations.

For the purposes of protecting the whistleblower, if the information disclosed falls within a prescribed category, it is irrelevant whether or not it is confidential. Those categories include:

- danger to the health and safety of any person
- criminal offence
- failure to comply with any legal obligation.

The FOM recognises that OH staff will have access to information that could be covered by the Act. It advises OH staff to look carefully at the Act and discuss the circumstances with the medical defence organisation or legal adviser before disclosing such information. Similarly, when OHNs are faced with situations that they feel must be reported, in spite of a request from colleagues/patients/clients for confidentiality, they are advised to consider the criteria of the Act carefully. Where necessary they should discuss situations with senior professionals, the NMC, their RCN steward or full-time RCN officer before taking further action.

# 9 Consent to disclosure

## Consent

In asking for consent to disclose information you must ensure that a patient/client knows:

- the exact details of the request
- the scope of the information
- what it will be used for
- with whom it will be shared
- that consent is freely given without inducement or coercion.

Where a patient/client agrees to information being disclosed then there will be no breach of confidence. Although a verbal consent is valid in law, you are strongly advised to obtain written consent. The OH professional should ensure that the patient/client understands exactly what information/documentation will be disclosed. For example, are you going to use the full medical record, an extract or a report.

The FOM suggests that:

"In communicating with managers on the health of employees, it will normally be appropriate only to refer to the results of the health assessment and not the clinical details."

para 2.2 *Ethics for occupational physicians*

In 2002 D'Auria looked at the issues raised by rejecting an applicant for employment on grounds that are subsequently found to be discriminatory. He reminds us that the 1995 Disability Discrimination Act makes it clear that where an employee's disability is known by an employer's agent, for example OH doctors and nurses, then the employer cannot later claim lack of knowledge, and use this as a viable defence against failure to make reasonable adjustments.

Case study three demonstrates the complexity of managing confidential information. It raises questions about protecting the confidences of the client/patient, and using informed consent to release information that might jeopardise employment opportunities.

From this case study it is clear that:

1. where the pre-employment health questionnaire provides that information given may be disclosed to the employer, and not simply be confined to the occupational health department, the job applicant's 'unqualified' completion of the questionnaire will give rise to no duty of confidentiality between him and the OH department
2. where the pre-employment health questionnaire states that any information given will be confidential, and maintained as such by the OH department, the employer will have no right to demand access to the information in the absence of the job applicant's consent. The duty of confidentiality will not be overridden by the Disability Discrimination Act 1995, 2005
3. OHNs should be explicit with job applicants about the purpose for which the questionnaire is being completed, and must ensure that they do not use the information disclosed for any other purpose.

It is therefore clear that OHNs must ensure that consent is sought and given for a specific purpose at a specific time and not used for carte-blanche purposes.

### Case study three

*London Borough of Hammersmith & Fulham* v *Farnsworth* [2000] IRLR 691

In *London Borough of Hammersmith & Fulham* v *Farnsworth* [2000] IRLR 691 Ms Farnsworth, who had a history of mental illness, applied for a social work post with the council. After consulting with Ms Farnsworth's GP and hospital doctor the council's occupational health physician reported to the council that she was concerned that Ms Farnsworth's ill-health might recur. She believed this would affect her performance and attendance at work. The council withdrew its provisional offer of employment, and Ms Farnsworth complained to an employment tribunal under the 1995 Disability Discrimination Act. Rejecting the council's appeal against the tribunal's finding of unlawful discrimination, the employment appeal tribunal (EAT) commented that the council's "self-denying" practice of not making enquiries of the OH physician about the job applicant's medical history was not justified. EAT referred to the duty of confidentiality owed by the employers to the job applicant. In this case the applicant had completed a consent form to disclose her medical history to the employer. In conclusion, the judgement makes it clear that it is wrong to plead a duty of confidence to prevent disclosure when a competent adult had explicitly given consent.

## Withholding consent

The NMC guidance says that if the patient/client withholds consent, or if consent cannot be obtained for whatever reason, disclosure may be made only where it can be justified in the public interest. This is usually where disclosure is essential to protect the patient/client or someone else from the risk of significant harm, or it is required by law, or by a court order.

The GMC accepts that confidentiality may be broken without consent when it is in the patient's interests and it is undesirable on medical grounds to ask for consent. This must be a rare event in employment and should only happen in exceptional circumstances.

It may not be possible to obtain consent where, for example, the patient is not legally competent. In these circumstances, the courts would probably accept that disclosure can take place provided the professionals involved judge it is in the patient's best interests (see *F* v *W Berkshire H A* [1989] 2 All ER).

### Scenario five
### Withholding consent

Nurse Brown worked in a large bakery. He had been supporting an employee who had developed severe breathlessness while working rotational shifts in the grain store. Pre and post–shift ventilation measurements clearly pinpointed exposure at work as the culprit. The nurse had explored the work situation and was satisfied that efficient and rigorous hygiene controls were in place. Meanwhile, the employee's breathlessness was worsening and it became increasingly clear that this was a case of occupational asthma. The nurse explained to the employee that he should have a full assessment, and that continued exposure to grain and flour might lead to permanent lung damage. At this point, the employee became adamant that the nurse must not give any information to his managers, personnel or his GP. He also refused the offer of a referral to the chest physician because he said he could not afford to come off shift work or lose his job.

**Facts**

- So far nurse Brown has maintained confidentiality. However, the nurse concludes that the health of the employee will continue to deteriorate and that over time he may have to leave his job completely.
- The NMC *Code of Professional Conduct* provides clear guidance on this issue. There are legitimate reasons to break confidentiality where not to do so might lead to the harm of the patient.
- If the illness is confirmed as a prescribed occupational disease such as occupational asthma, the Health and Safety Executive would be required to investigate the circumstances.

**Conclusions**

- The employee should be given as much information as possible about the potential risk to health, and the consequences of continued exposure by refusing temporary redeployment or referral for medical investigation.
- The nurse should be optimistic but honest in his appraisal of the potential consequences. It may be that the employee has to be moved permanently from the grain store and be redeployed into day work.
- If the employee still refuses to give permission for the nurse to discuss adjustments, redeployment or medical investigations, the nurse is faced with a serious decision because ultimately the employee may not be able to continue in his job.
- The nurse should discuss such a decision with the NMC and RCN before deciding to disclose, and carefully record his actions.
- The nurse may be able to reassure the employee that full clinical details need not be given to management. The advice given can be confined to the need for adjustments/redeployment data.

## Access to information during court proceedings

If an OH professional is required to give evidence in any court proceedings, then they cannot withhold confidential information. If information is withheld it is contempt of court and punishable as a criminal offence. However, a professional can ask the judge permission to decline to answer a question about a confidential matter. It will be up to the judge to decide whether the information should be disclosed (*D* v *NSPCC* [1978] AC 171).

In very limited circumstances, information may be withheld from the court on the ground of 'legal professional privilege'. Only communications between a client and his legal adviser, or between a third party and the client or his lawyer, where they were made in contemplation of litigation, and the dominant purpose was to prepare for the litigation, may be withheld from the court. Accordingly, a party to legal proceedings may withhold a report obtained from an OH professional for the purposes of litigation, where the client decides not to rely on its content.

An employer's investigation into an accident at work that is conducted both because the employer wants to ensure that there is no repetition, and because it anticipates court proceedings (litigation), is not privileged (*Waugh* v *British Rail* [1980] AC 521).

Where an employee is involved in litigation against an employer, perhaps for personal injury allegedly caused during the course of his work, the employer has no automatic right to access the employee's OH records. In the absence of the employee's consent, the lawyers acting for the employer will need to seek from the court an order for disclosure.

### Case study four

*Dunn* v *British Coal Corporation* [1993] ICR 59

An appeal court accepted that occupational health records were confidential between the doctor and employee, and that where an employer was threatened with legal action by the employee, neither the employer nor its legal advisers were entitled to see the health records in the absence of the employee's consent.

A coroner's court has the power to order disclosure of medical records and other confidential medical information. This is usually by a high court subpoena (a writ that demands records or the appearance of a person in court) (*R* v *Southwark Coroner ex parte Hicks* [1987] 1 WLR 1624).

Health and safety inspectors have extensive powers under section 20 of the 1974 Health and Safety at Work Act (HSWA 74). This includes the right to require the production and inspection of books or documents that are relevant to the investigation, and to take copies of them. No exemption applies in respect of medical reports or records. The inspector may also require any person who has information relevant to the investigation to answer questions. It is an offence (under section 33 HSWA 74) to contravene any requirement imposed by an inspector.

In a civil action in the courts, access to medical reports and records may be essential, particularly in personal injury or medical negligence claims. A court can make an order requiring the pre-action disclosure of documentary evidence by a prospective party (section 34 Supreme Court Act 1981; section 53 County Courts Act 1984; Civil Practice Rules, Parts 25.1(I) and 31.16).

During the course of litigation a party to the court proceedings may use the Civil Practice Rules (Parts 31.5 and 31.6) to obtain a disclosure order for otherwise confidential medical information under. An order for disclosure against someone who is not party to the court proceedings may be obtained under Part 31.17.

Where appropriate, the court can order that disclosure is made to the patient's advisers, but not the patient. For example, look at section 33(2) of the 1981 Supreme Court Act. The court has no power to prevent the patient's lawyers receiving the documents. Legal professional privilege may apply in any event.

Public interest immunity may prevent disclosure of otherwise relevant and material documentation. For example, see *R* v *Chief Constable of West Midlands, ex parte Wiley* [1994] 3 WLR 433. Medical documents may attract this immunity as can be seen in *R* v *Secretary of State for the Home Department, ex parte Benson*, unreported, 1 November 1988, cited in *R* v *Secretary of State for the Home Department, ex parte Duggan* [1994] 3 All ER 277.

## Scenario six
### Pressure from employers

Nurse Black is employed by the chemical company ChemComp. He is asked by a member of senior management to send the health records of an employee who has taken out a personal injury claim against the company. The nurse refuses because he does not have consent from the employee. The manager puts pressure on the nurse by telling him that the records legally belong to the company and that he has no right to withhold access.

**Facts**

- Certain rules of disclosure apply to personal injury claims that require documents to be disclosed to both plaintiff and defendant. In such cases records would be requested by a court.
- Pressure on the nurse can be intense when senior management demand access.

**Conclusions**

- Nurses should ask for job descriptions that make the boundaries of confidentiality explicit and that recognises the NMC Professional Code of Conduct in the terms and conditions of employment.
- The nurse should inform management that in the absence of consent from the client or a court order they are unable to give access to confidential OH records because this would be in breach of their Professional Code of Conduct.
- If continued and inappropriate pressure is placed on the nurse to provide access to OH records in the absence of consent or a court order, RCN and/or NMC advice should be taken.
- The nurse should carefully record all events and actions.

# 10 Statutory provisions

**There are now a number of statutory provisions that require disclosure of information to a public body (and/or confirm the strict nature of the duty of confidentiality). They include the following:**

**Abortion Act 1967** requires doctors to give the Chief Medical Officer notice of pregnancy terminations, including the name and address of the woman concerned.

**Health and Safety at Work Act 1974** and Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 require the reporting of dangerous occurrences to the local authority or Health and Safety Executive. These incidents are, for example: events that could have led to serious injury which was averted; major accidents such as fractures, amputation, loss of consciousness and so on; minor accidents causing incapacity for more than three days; and industrially linked diseases such as hepatitis contracted while working with human blood products. Occupational health professionals should resist any request by the employer that they take responsibility for reporting accidents and disease, as this may give rise to a conflict of interest between the professional's relationship with the employer and that with the patient/employee.

We have already said that health professionals are under no obligation to disclose confidential information to assist the police in a criminal investigation. There are some statutory exceptions, and the BMA has also suggested that doctors should consider informing the police only:

- where the offence is grave
- the prevention or detection of the crime will be seriously delayed or prejudiced if they do not do so
- the information will only be used in the detection and prosecution of the alleged offender (*Philosophy and practice of medical ethics* 1988, 23 – 4).

The Department of Health gives similar advice on disclosing information to the police. You can find this advice in the *Code of Practice on Confidentiality (2003)*.

**Misuse of Drugs (Notification of and Supply of Addicts) Regulations 1973** impose an obligation on doctors treating drug addicts to send the Chief Medical Officer at the Home Office details of people who they consider, or suspect are addicted to certain controlled drugs

**National Health Service (Venereal Diseases) Regulations 1974** require every health authority to take all necessary steps to secure information that could identify an individual who has or is receiving treatment for any sexually transmitted disease. This information should not be disclosed except for the purpose of communicating the information to a doctor or someone working under his direction in connection with the treatment of persons suffering from the disease or the prevention of its spread.

**Police and Criminal Evidence Act 1984** permits specific access in a criminal investigation to what is called excluded material. Section 11 defines excluded material as, for example, "human tissue or tissue fluid which has been taken for the purposes of diagnosis or medical treatment and which a person holds in confidence". Section 12 permits access to personal records, which relate to an individual's physical or mental health. However, an order for the seizure of personal records can only be made in limited circumstances, and only by a circuit judge (not with a magistrate's warrant). The order gives the right to enter premises and search for the personal records.

**Public Health (Control of Diseases) Act 1984** (supplemented by the Public Health (Infectious Diseases) Regulations 1988) requires the notification of certain diseases to the local authority. They include: cholera; plague; small pox; typhus; acute meningitis; relapsing fever; TB; whooping cough; and food poisoning etc. For this purpose, AIDS is not a notifiable disease.

**Road Traffic Act 1988** obliges anyone, including health care professionals, to provide the police, on request, with any information that might identify a driver who is alleged to have committed a traffic offence.

**Note:** There is no obligation on health professionals to disclose confidential information in order to assist the police with the investigation of crimes (*Sykes* v *DPP* [1962] AC 528). You do not "obstruct" police investigations by refusing to answer their questions, provided that you have "lawful excuse". Confidentiality would constitute a "lawful excuse" (*Rice* v *Connelly* [1966] 2 All ER 649).

**Terrorism Act 2000** requires anyone to disclose to the police, as soon as possible, any information that they may have that may help prevent an act of terrorism or assist in apprehending or prosecuting such terrorists.

11

# Access to information for medical audit or research

There is no clear legal authority for disclosure of confidential health information for medical audit or research. However, it may be justified in the public interest, in the absence of the patient's consent. In general, the normal principles discussed above should apply. In other words, the patient or client should know who is asking for access to their records, and for what purpose, and they should be afforded the opportunity to deny access if they wish.

Confidentiality and disclosure for research purposes were explored by the courts in *R* v *Department of Health ex parte Source Informatics Ltd* (2000) Lloyd's Med Rep 76. The Court of Appeal ignored whether anonymised information was still confidential, and simply asked whether the researchers had acted unconscionably.

A data collecting company approached GPs for their consent to obtain patient treatment information. The DH advised that the patient would not have entrusted the information to either the GP or the pharmacist to give to the data company. Further, it maintained that disclosure of dispensing information to data companies could not be argued to be in the public interest. The judge accepted that there would be a breach of confidence if the company were given access to the confidential information given by the patient to the pharmacist.

The case went to a Court of Appeal where the first ruling was overturned, The court held that there was no breach of confidence where the identity of the person concerned is protected. After reviewing the legal authorities on confidentiality, Lord Justice Simon Brown commented:

"… the one clear and consistent theme emerging from all these authorities is this: the confidant is placed under a duty of good faith to the confider and the touchstone by which to judge the scope of his duty and whether or not it has been fulfilled or breached is his own conscience, no more and no less…. The concern of the law is to protect the confider's personal privacy".

The GMC guidance makes clear that where patients or clients could be identified from the information their consent should be obtained first, and their refusal respected (*Confidentiality* paras 15 and 17).

While the BMA advises that wherever possible research should use anonymised data, and, where this isn't possible, the patient's explicit consent should be sought. All such research must be subject to approval by a research ethics committee, within or outside the NHS, although the approval should not alone be sufficient to justify a breach of confidentiality (*Medical Ethics Today,* 2nd edtion, 2004).

Similarly, occupational health nurses and nursing students must obtain permission from an ethics committee before undertaking research in the NHS that involves patients/clients or access to confidential information where individuals can be identified. Increasingly, student research requests are being denied due to the complexity of ensuring informed consent, and because of an increasing number of requests.

In non-NHS settings, in the absence of ethical approval from a committee, the manager of the OH service is responsible for the security of the information contained in the records and for making sure that access to the information is appropriate and is closely supervised.

Section 60 of the Health and Social Care Act 2001 enables the Secretary of State for Health to make regulations about processing patient information for medical interest. This is on the basis that to do so is either in the interests of improving patient care or in the public interest.

In May 2002 the Information Commissioner (who enforces the DPA) issued guidance on *The use and disclosure of health data.* This explains the commissioner's views on the research exemption to the data protection principle.

Overall, it is clear, that OH professionals must ensure that group data obtained for screening or monitoring purposes, or the preparation of management reports, does not and cannot reveal the identity of the individuals in it.

Good practice also includes giving information to patients/clients about how grouped data may be used and why, and a record made that consent has been given.

12

# Appendix 1

## References

British Medical Association (1984) *Handbook of medical ethics,* London: BMA

British Medical Association (1993) *Medical ethics today*, London: BMA

British Medical Association (1998) *Philosophy and practice of medical ethics*, London: BMA

D'Auria, D (2002) Are pre-employment health questionnaires confidential? *Occupational Health Review*, July/August, pp 37 – 40.

Department of Health (1996) *The protection and use of patient information*, London: DH

Department of Health (1994) *AIDS/HIV – infected health care workers: guidance on the management of infected health care workers*, London: DH (Expert Advisory Group revised December 1998 and 2002)

Department of Health (2003) *Code of practice on confidentiality*, London: DH

Department of Health (2000) *Hepatitis B infected health care workers – HSC 2000/020*, London: DH, www.dh.gov.uk

Department of Health (2002) *Hepatitis C infected health care workers – HSC 2002/010*, London: DH, www.dh.gov.uk

The Institute of Medical and Biological Illustration (1988) *Code of practice on confidentiality of illustrative clinical records*, London: IMBI

General Medical Council (1995) *Duties of a doctor*, London: GMC

General Medical Council (1995) *Confidentiality*, London: GMC

General Medical Council (1995) *HIV and AIDS: the ethical considerations*, London: GMC

General Medical Council (1998) *Seeking patients consent: the ethical considerations*, London: GMC

Kloss, D (2001) *Occupational health law 3rd edition*. Oxford: Blackwell Science Publishing, www.blackwell-science.com

Nursing and Midwifery Council (2002) *The Code of Professional Conduct*, London: NMC

Office of the Information Commission (2005) *Employment Practice Code*, London OIC www.informationcommissioner.gov.uk

D. Wright (1999) *Guidance on Ethics for Occupational Physicians* (5th edition), London: FOM www.jacocomed.as.uk

## Further reading

Data Protection (2002) *Notification exemptions: a self-assessment guide*, Cheshire: Office of the Information Commissioner

Data Protection (2001) *Notification handbook: a complete guide to notification*, Cheshire: The Office of the Information Commissioner

Data Protection (2000) *Draft code of practice: the use of personal data in employer/employee relationships*, Cheshire: Office of the Information Commissioner

# Appendix 2

## UK Government acts and regulations


Health and Safety Executive (1995) *The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations*, Sudbury: HSE

Parliament (1967) *The Abortion Act*, London: HMSO

Parliament (1988) *Access to Medical Reports Act*, London: HMSO

Parliament (1990) *Access to Health Records Act* (replaced by Data Protection Act 1998), London: HMSO

Parliament (1998) *The Data Protection Act*, London: HMSO

Parliament (1995) *The Disability Discrimination Act* (updated 2005), London: HMSO

Parliament (1974) *The Health and Safety at Work Act*, London: HMSO

Parliament (2001) *The Health and Social Care Act*, London: HMSO

Parliament (1998) *The Human Rights Act*, London: HMSO

Parliament (1973) *The Misuse of Drugs (Notification of and Supply of Addicts) Regulations*, London: HMSO

Parliament (1974) *The National Health Service (Venereal Diseases) Regulations*, London: HMSO

Parliament (1984) *The Police and Criminal Evidence Act*, London: HMSO

Parliament (1989) *The Prevention of Terrorism (Temporary Provisions) Act* (replaced by The Terrorism Act 2000), London: HMSO

Parliament (1984) *The Public Health (Control of Diseases) Act*, London: HMSO

Parliament (1998) *Public Interest Disclosure Act*, London: HMSO

Parliament (2000) *The Terrorism Act*, London: HMSO


# Appendix 3

## Useful contacts

**Royal College of Nursing**
20 Cavendish Square
London
W1G 0RN

Telephone 020 7409 3333
www.rcn.org.uk

RCN Direct
Telephone 0845 772 6100

**Nursing and Midwifery Council**
23 Portland Place
London
W1B 1PZ

Telephone 020 7637 7181
Fax 020 7436 2924
www.nmc-uk.org

**Office of the Information Commissioner**
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Switchboard: 01625 545 700 Fax: 01625 545 700
www.informationcommissioners.gov.uk

**General Medical Council**
178 Great Portland Street
London
W1W 5JE

Telephone: 020 758 7642
www.gmc-uk.org

**Faculty of Occupational Medicine**
Royal College of Physicians
6 St Andrews Place
London
NW1 4LE

Telephone: 020 7317 5890
www.facoccmed.ac.uk

Royal College of Nursing

**October 2003, revised October 2005**

Published by the
Royal College of Nursing
20 Cavendish Square
London
W1G 0RN

020 7409 3333

**RCN ONLINE**
**www.rcn.org.uk**

**RCN DIRECT**
www.rcn.org.uk/direct
**0845 772 6100**

The RCN represents nurses and nursing, promotes excellence in practice and shapes health policies.

Publication code 002 043

CONFIDENTIALITY