Confidentiality and disclosure of health information tool kit



BMA

Contents

Card 1 **5**
Guidance on confidentiality

Card 2 **8**
General information

Card 3 **14**
Sources of confidentiality rights and protections

Card 4 **19**
Security of information

Card 5 **23**
Recordings, publication and the media

Card 6 **27**
Assessment of capacity and determining 'best interests'

Card 7 **30**
Adults who lack capacity

Card 8 **34**
Children and young people

Card 9 **39**
Legal and statutory disclosures

Card 10 **44**
Public interest

Card 11 **49**
Deceased patients

Card 12 **51**
Serious communicable diseases

Card 13 **53**
Secondary uses of patient information

Card 14 **55**
Uses of information for non-medical purposes

Card 15 **57**
Dual responsibilities

Card 16 **60**
Useful names and addresses

About this tool kit

Questions about confidentiality and disclosure of health care information are a significant area of ethical enquiry for the British Medical Association (BMA) and the volume of queries exceeds other issues of ethical concern raised by BMA members. While health professionals are aware of their traditional obligations to protect confidentiality, they also recognise that ever more complex dilemmas arise from that duty. Queries around confidentiality and disclosure are becoming more complicated. There is an ever growing list of demands on health professionals to disclose information to third parties such as insurers, the police, social workers, the DVLA and the relatives of deceased patients. There is also growing concern over the implications of increased access to patient information by electronic means and the use of patient information for secondary uses such as audit, commissioning, payment by results, research and teaching.

The purpose of this tool kit is not to provide definitive answers for every situation but to identify the key factors which need to be taken into account when such decisions are made. The tool kit consists of a series of cards about specific areas of confidentiality relating to children, adults who lack capacity and the deceased as well as the secondary uses of information. Separate cards have been produced identifying factors to be considered when assessing competence and determining 'best interests', security of information and the sources of confidentiality rights and protection. All cards refer to useful guidance from bodies such as the General

Medical Council (GMC), BMA and health departments, that should be used in conjunction with the cards. In addition, the medical defence bodies and many of the Royal Colleges produce specific advice for their members: Card 16 lists contact details for organisations from whom further advice can be obtained.

The tool kit is available on the BMA's website and individual Trusts, medical schools and individual health professionals may download and adapt it to suit their own requirements. There are no copyright restrictions on this tool kit – please feel free to make multiple copies.

The BMA would welcome feedback on the usefulness of the tool kit. If you have any comments please address them to:

Medical Ethics Department
British Medical Association
BMA House
Tavistock Square
London WC1H 9JP
Tel: 020 7383 6286
Fax: 020 7383 6233
Email: ethics@bma.org.uk
Website: www.bma.org.uk

This is the first edition of the BMA's *Confidentiality and disclosure of health information tool kit*. Information about developments since its publication may be obtained from the BMA's website or by contacting the BMA Medical Ethics Department.

CARD 1

Guidance on confidentiality

Publication	Abbreviation on other cards used
0-18 Years: Guidance for all Doctors General Medical Council (2007)	'0-18 Years'
Access to Health Records by Patients British Medical Association (2007)	'Access'
Assessment of Mental Capacity British Medical Association and The Law Society (1995 – 3rd edition due in December 2009)	'Capacity'
Code of Practice on Protecting the Confidentiality of Service User Information Northern Ireland Department of Health, Social Services and Public Safety (2009)	'NI Confidentiality'
Confidentiality: NHS Code of Practice Department of Health (2003)	'DH Code'
Confidentiality: Protecting and Providing Information General Medical Council (2009)	'GMC'
Consent, Rights and Choices in Health Care for Children and Young People British Medical Association (2001)	'Children'

Guidance on the Secondary Uses of Patient Information
British Medical Association (2007) 'SU'

Handling Confidential Patient Information in Contracting
Department of Health (1992) 'Contracting'

Information about Patients: An Introduction to the Patient Information Advisory Group for Health Professionals and Researchers
Patient Information Advisory Group (2006)
In 2009 PIAG was re-named the Ethics and Confidentiality Committee (ECC). 'ECC'

Information Security Management: NHS Code of Practice
Department of Health (2007) 'Security'

Making and Using Visual and Audio Recordings of Patients
General Medical Council (2002) 'Recordings'

Medical Ethics Today: The BMA's Handbook of Ethics and Law
British Medical Association (due to be updated 2009) 'MET'

Medical Treatment For Adults With Incapacity: Guidance On Medico-Legal Issues in Scotland
British Medical Association (2009) 'Scotland Incapacity'

NHS Chaplaincy: Meeting the Religious and Spiritual Needs of Patients and Staff
Department of Health (2003) 'Chaplaincy'

NHS Code of Practice on Protecting Patient Confidentiality Scottish Government Health Directorates (2003) 'Scotland Confidentiality'

Records Management: NHS Code of Practice
Department of Health (2006) 'Records Management'

The Caldicott Guardian Manual
Department of Health (2006) 'Caldicott'

The Impact of the Human Rights Act 1998 on Medical Decision-Making
British Medical Association (2007) 'HRA'

The Mental Capacity Act – Guidance for Health Professionals
British Medical Association (2007) 'MCA'

Use and Disclosure of Health Data
Information Commissioner (2002) 'IC'

CARD 2

General information

1. The duty of confidentiality

Confidentiality is an essential requirement for the preservation of trust between patients and health professionals and is subject to legal and ethical safeguards. Patients should be able to expect that information about their health which they give in confidence will be kept confidential unless there is a compelling reason why it should not. There is also a strong public interest in maintaining confidentiality so that individuals will be encouraged to seek appropriate treatment and share information relevant to it.

2. What is confidential?

All identifiable patient information, whether written, computerised, visually or audio recorded or simply held in the memory of health professionals, is subject to the duty of confidentiality. It covers:

- any clinical information about an individual's diagnosis or treatment
- a picture, photograph, video, audiotape or other images of the patient
- who the patient's doctor is and what clinics patients attend and when
- anything else that may be used to identify patients directly or indirectly so that any of the information above, combined with the patient's name or address or full postcode or the patient's date of birth, can identify them.

Even where such obvious identifiers are missing, rare diseases, drug treatments or statistical analyses which have very small numbers within a small population may allow individuals to be identified. A combination of items increases the chance of patient identification.

Whilst demographic information such as name and address are not legally confidential, it is often given in the expectation of confidentiality. Health professionals should therefore usually seek patient consent prior to sharing this information with third parties.

3. Using and disclosing information

From time to time, the duty to preserve confidentiality can present health professionals with an ethical or legal dilemma, commonly when a third party requests information about patients or their treatment. A number of factors must be considered including:

- patients must be properly informed as to how identifiable information about them is used
- data should be anonymised wherever possible
- explicit consent should be sought for the use or disclosure of personal health information, unless it is clearly implied
- occasionally, when it is not practicable to obtain consent, information may be disclosed where the law requires or where there is an overriding public interest, eg where child abuse is suspected
- disclosures should be kept to the minimum necessary to achieve the purpose

- when patients withhold consent to disclosure of their information, their wishes should be respected
- health professionals must always be prepared to justify their decisions about the use of personal health information.

4. Consent

Consent to disclosure may be explicit or implied. It may also be consent to disclosure of specific information to a particular person or body for a particular purpose or it may be consent to general future disclosure for particular purposes. In either case consent should be informed and freely given.

Explicit or express consent is achieved when a patient actively agrees, either orally or in writing, to a particular use or disclosure of information which has been discussed with the patient. Explicit consent is the ideal as there is no doubt as to what has been agreed.

Patient agreement can also be implied, signalled by the behaviour of an informed patient. Implied consent is not a lesser form of consent but in order for it to be valid it is important that patients are made aware that information about them will be shared, with whom it will be shared, and of their right to refuse. Health professionals bear responsibility for the disclosures they make, so when consent is taken to be implied, they must be able to demonstrate that the assumption of consent was made in good faith and based on good information. If not, it is no consent at all and some other justification will be needed for its

disclosure. In addition to information provided face to face in the course of a consultation, leaflets, posters and information included with an appointment letter from a hospital or clinic can play a part in conveying to patients the reality and necessity of information sharing. Clearly, a combination of methods provides greater security that patients have understood. It should be noted that the more sensitive and detailed the data, the more likely it is that explicit consent will be required, eg sexual health information.

5. Anonymisation

Information may be used more freely if the subject of the information is not identifiable in any way. Usually, data can be considered to be anonymous where clinical or administrative information is separated from details that may permit the individual to be identified such as name, date of birth and postcode. Even where such obvious identifiers are missing, rare diseases, drug treatments or statistical analyses which have very small numbers within a small population may allow individuals to be identified. A combination of items increases the chances of patient identification. When anonymised data will serve the purpose, health professionals must anonymise data to this extent and, if necessary, take technical advice about anonymisation before releasing data. Whilst it is not ethically necessary to seek consent for the use of anonymised data, general information about when their data will be anonymised should be available to patients.

6. Pseudonymisation

Pseudonymisation is sometimes referred to as reversible anonymisation. Patient identifiers, such as name, address or NHS number, are substituted with a pseudonym, code or other unique reference so that the data will only be identifiable to those who have the code or reference. Where those who are using data have no means to reverse the process, and so no way to identify an individual from the data they have, the data may be treated as anonymised and there is no common law requirement to seek consent for their use. For those who have access to both pseudonymised data and the means to reconstitute them, they should be treated as identifiable. The use of pseudonymised data is common in research. As with anonymised data, patients should generally be informed when it is intended that their information will be pseudonymised.

7. Sharing information with other health professionals

In the absence of evidence to the contrary, patients are normally considered to have given implied consent for the use of their information by health professionals for the purpose of the care they receive. Information sharing in this context is acceptable to the extent that health professionals share what is necessary and relevant for patient care on a 'need to know' basis. Health and social care, although often closely related, do not always fall into the same category, and disclosure of information to social services usually requires explicit consent from competent patients. Sometimes two competing interests come into

conflict, such as the patient's informed refusal to allow disclosure and the need to provide effective treatment to that person. A patient's refusal to allow information-sharing with other health professionals may compromise patient safety, but if this is an informed decision by a competent person it should be respected.

8. Multi–agency working

Health professionals during the course of their treatment of patients will have contact with partner organisations from time to time. These include social services and housing and benefits agencies. In community settings many integrated teams have been established, which include workers from health, social services and non-statutory bodies. Health professionals should from the outset discuss with patients the desirability of sharing information with other agencies where appropriate. Other agencies may wish to be involved in discussions about patients at various points in their treatment or to attend case conferences or multi-disciplinary meetings. Health professionals may also be invited to attend external case conferences organised by partner organisations to discuss the health and welfare of patients. In all these circumstances confidential information should be shared with explicit consent or, in the absence of consent, where disclosure is required by law or there is an overriding public interest in disclosure.

(See also Card 1: 'DH Code', 'GMC', 'IC', 'MET', 'NI Confidentiality', 'Scotland Confidentiality' and 'ECC'.)

CARD 3

Sources of confidentiality rights and protections

It is important to note that the ethical, professional, contractual and legal positions on confidentiality are complex. For example, the legal responsibilities in respect of confidential information cannot be gleaned from common law and statute alone, and health professionals must look at the overall effect of the law, not each aspect in isolation. In terms of statute, the Data Protection Act sets out circumstances in which the use of data may be lawful. The common law generally requires consent for disclosure. Health professionals must be sure that any use of data falls into the relevant Data Protection Act categories and meets the common law requirement for consent except where disclosures are required by law or in the public interest. Health professionals who are uncertain about the application of the law should seek legal advice. They must also ensure that their actions comply with the guidance issued by their regulatory body and their employers.

The use of information about individual patients is governed by the following:

1. Contract of employment

Confidentiality of patient information is a requirement of employment under NHS and many independent sector contracts. All staff employed by or contracted to the NHS may be disciplined following a breach of patient confidentiality.

2. Professional standards

All health care professionals must maintain the standards of confidentiality laid down by their professional body, such as the GMC, or risk complaint for professional misconduct. This may result in a warning, restriction of practice or removal from the register. (See also Card 1: 'GMC'.)

3. Policies and organisational standards

A wide range of policies and standards exist which provide guidance for health professionals to ensure that patients are fully involved with decisions about the use of their information and that information provided by patients is kept confidential. This includes the Caldicott Guardian Manual (2006), the Department of Health Confidentiality: NHS Code of Practice (2003), the Scottish Government Health Directorates NHS Code of Practice on Protecting Patient Confidentiality (2003), and the Northern Ireland Code of Practice on Protecting the Confidentiality of Service User Information (awaiting publication).

4. NHS Care Record Guarantee

The NHS Care Record Guarantee emphasises the commitment of the NHS in England to the confidentiality and security of patient information. The guarantee covers:

- patients' access to their own records
- controls on access by others
- how access will be monitored and policed
- options patients have to further limit access
- access in an emergency
- what happens when patients cannot make decisions for themselves.

5. Data Protection Act 1998

The Data Protection Act regulates the processing of information about living individuals, such as obtaining, use or disclosure of information. It covers paper and computer records. Patients are entitled to be informed that information is being held about them and of the purposes for which their information will be processed. They are entitled to have access to and a copy of their information, except where there are grounds for believing that access to that information would be likely to cause serious harm to the individual or a third party or where it would entail disclosure of another individual's identifiable data. They are also entitled to have information corrected when it is inaccurate. (See also Card 1: 'IC' and 'Access'.)

6. Access to Health Records Act 1990

The Data Protection Act does not cover the records of deceased patients. Statutory rights of access are contained within the Access to Health Records Act 1990 and Access to Health Records (Northern Ireland) Order 1993. A personal representative or any person with a claim arising from the death of a patient has a right of access to information directly relevant to the claim. Information which is not directly relevant to the claim may not be released. (See also Card 1: 'Access'.)

7. Human Rights Act 1998

A right to 'respect for private and family life' is guaranteed in article 8 of the Human Rights Act (HRA). This right is not absolute, and may be derogated from where the law permits and 'where necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others'. The effect is similar to that of the common law: privacy is an important principle which must be respected, but may be breached where other significant interests prevail. Any such breach must be proportionate to the benefits/harms it is intended to bring/avoid. (See also Card 1: 'HRA'.)

8. Computer Misuse Act 1990

It is an offence under the Act to gain unauthorised access to computer material. This would include using another person's ID and password without authority in order to use, alter or delete data.

9. NHS Act 2006

In England and Wales, Section 251 of the NHS Act 2006 gives the Secretary of State for Health power to make regulations permitting the disclosure of identifiable information without consent in certain circumstances. Health professionals can apply to the Ethics and Confidentiality Committee (ECC), an independent public body which advises the Secretary of State for Health in England and Wales about the lawful basis for disclosure of patient-identifiable information. (See also Card 1: 'ECC'.)

10. The common law

The common law is based on previous judgments in court. Whilst various interpretations of the common law may be possible, there is widespread acceptance that it reinforces the view that information may be disclosed with patient consent, where there is an overriding public interest or where the law requires it. (See also Card 9 on Legal and Statutory Disclosures and Card 10 on Public Interest.)

CARD 4

Security of information

1. Keeping information secure

Protection is needed against both external threats such as theft and internal threats such as inappropriate access by staff. Health professionals should not leave computers, medical records or files unattended in the workplace. Ideally, all records and laptops should be kept in a locked environment. Health professionals should not normally take records or laptops containing electronic information out of the workplace. Where this cannot be avoided, for example if it is necessary to take records on visits to patients' homes, procedures for safeguarding the information should be in place. Discussion about clinical management of patients should be kept confidential and out of earshot of those not involved in their care and especially the public. All people who come into contact with personal health information in their work should have training in confidentiality and security issues.

Health professionals who are also employers should ensure that employees are aware of their ethical, legal and contractual duty of confidentiality and how to keep information secure within their health setting. (See also Card 1: 'Security'.)

2. All records

For all types of records health professionals should:

- never inappropriately access records
- shut/lock doors, offices and filing cabinets
- wear ID if issued
- query the status of visitors/strangers
- not tell unauthorised personnel how the security systems operate
- advise senior personnel if anything suspicious or worrying is noted
- confirm the identity of telephone callers.

3. Manual records

Manual records should be:

- held in secure storage
- booked out from their normal filing system
- tracked if transferred, with a note of their current location within the filing system
- returned to the filing system as soon as possible after use
- stored closed when not in use so that the contents are not seen by others
- inaccessible to members of the public
- kept on site unless removal is essential.

4. Electronic records

In the case of electronic records health professionals should:

- always log out of any computer system or application when work is finished
- not leave a terminal unattended and logged in
- not share Smartcards or passwords with others
- change passwords at regular intervals to prevent others using them
- always clear the screen of a previous patient's information before seeing another.

5. Email and fax

In the case of email and fax:

- health professionals should be satisfied that there are appropriate arrangements for the security of personal information when it is stored, sent or received by fax, computer, email or other electronic means
- whenever possible, clinical details should be separated from demographic data
- all data transmitted by email should be encrypted
- when information is being transmitted by fax, it is sensible to enquire whether the receiving machine is in a publicly accessible area, such as a waiting room, or in a private office, as information must only be transmitted when the receiving machine is known to be secure both during and out of working hours. Wherever possible, it should be confirmed after transmission that the intended recipient has collected the information. Where it is necessary to transmit particularly sensitive patient information to other health professionals, it may be appropriate to consider other, more secure, means of communication. (See also Card 1: 'Contracting'.)

6. Data retention and disposal

The health departments give detailed advice about the minimum retention periods applicable to NHS records. The recommendations apply to both electronic and manual records, and the BMA advises private practitioners to follow the same rules. When health professionals are responsible for destroying health records, they must ensure that the method of destruction is effective and does not compromise

confidentiality. Incineration, pulping and shredding are appropriate methods of destroying manual records. Electronic data should be destroyed using appropriate data destruction software. (See also Card 1: 'Records Management'.)

CARD 5

Recordings, publication and the media

1. Video and audio recordings and photographs

Recordings and photographs made for clinical purposes are part of the medical records, and are subject to the same duty of confidentiality. The GMC advises that it is necessary to obtain the consent of the patient or, in the case of a child who is unable to give consent, to obtain consent from someone with parental responsibility prior to a recording or photograph being made. In relation to adults lacking capacity, video and audio recording should only take place if it is in the patient's best interests. They should only be used for the purpose for which consent was granted, and must be stored securely. Clinical recordings should not be used for teaching purposes without consent if the patient is identifiable.

2. CCTV and surveillance

CCTV equipment should only be installed for a specific purpose, such as for the prevention and detection of crime. Patients using health care facilities should be made aware by notices if surveillance cameras are in use in public areas of GP surgeries and hospitals. The Information Commissioner provides guidance on the use of CCTV and the standards that should be followed. Disclosure of CCTV footage may take place, for example, to the police where it is justified in the 'public interest' but care must be taken to ensure that only relevant images are disclosed.

The BMA and GMC have particular concerns about the use of covert surveillance on health care facilities and the GMC states that doctors 'must obtain permission to make, and consent to use, any recording made for reasons other than the patient's treatment or assessment'. There are a few exceptions in which covert surveillance is acceptable, for example, in an in-patient setting where there are grounds to suspect relatives or carers of causing injury to a child, in which case legal advice should be sought and the involvement of police and social services agreed.

3. Out of hours service

Calls to an out of hours service are confidential and patients should be informed that their call may be recorded. The recording forms part of the patient's medical record and is accessible under the Data Protection Act. No call from a patient should be secretly recorded.

4. Television, radio, internet and print

The written consent of the patient or, in the case of a child who is unable to consent, written consent from someone with parental responsibility is required for all publications or recordings for broadcast or use in media to which the public will have access, including medical journals. This applies whether or not the patient is likely to be identifiable. Patients need to be informed that once they have agreed to the publication or recording, they may not be able to withhold their consent for its subsequent use. In relation to adults lacking capacity the law is untested. In the BMA's view it is difficult to see how such publications or recordings

could be in the individual's best interests. Before making any arrangements for individuals or organisations to film patients in a health care setting, permission should be sought, where appropriate, from the employing or contracting body and the organisation in which patients are being treated if this is different.

5. The press

Under normal circumstances there will be no basis for disclosure of confidential and identifiable information to the press. There will be occasions, however, when health professionals are asked for information about individual patients:

- comment on the condition of a celebrity patient. When the patient has the capacity to make decisions about disclosure, consent is essential before any information is released to the media. When the patient lacks capacity, legal advice should be sought
- after incidents involving harm to many people. During or after major disasters, for example a fire, road traffic accident, terrorist attack or outbreak of infectious disease, it is important that requests for information are dealt with sensitively, while not breaching the confidentiality of patients. It will not usually be necessary to give identifying or detailed clinical information about the people involved
- where a patient or a patient's relatives use the press as a vehicle to complain about the treatment and care provided. Many health professionals feel strongly that patients forfeit their rights to confidentiality by going to the press, and that they should be entitled to 'set the

record straight' and correct any inaccuracies. In practice health professionals who do this would risk criticism and breach confidentiality if the patient does not give consent. Where misleading information has been presented to the press, health professionals who wish to respond should limit their comments to pointing out that the information is inaccurate or incomplete.

(See also Card 1: '0-18', 'Children', 'Capacity', 'MCA', 'MET', 'Scotland Incapacity' and 'Recordings'.)

CARD 6

Assessment of capacity and determining 'best interests'

1. Are adults presumed to have capacity?

All people aged 16 and over are presumed, in law, to have the capacity to give or withhold their consent to disclosure of confidential information unless there is evidence to the contrary. A patient who is suffering from a mental disorder or impairment does not necessarily lack the capacity to give or withhold their consent. Equally, patients who would otherwise be competent may be temporarily incapable of giving valid consent due to factors such as extreme fatigue, drunkenness, shock, fear, severe pain or sedation. The fact that an individual has made a decision that appears to others to be irrational or unjustified should not be taken on its own as conclusive evidence that the individual lacks the mental capacity to make that decision. If, however, the decision is clearly contrary to previously expressed wishes, or is based on a misperception of reality, this may be indicative of a lack of capacity and further investigation will be required.

2. Are children and young people presumed to have capacity?

There is no presumption of capacity for people under 16 in England, Wales and Northern Ireland and those under this age must demonstrate their competence by meeting certain standards set by the

courts. The central test is whether the young person has sufficient understanding and intelligence to understand fully what is proposed. In Scotland, anyone aged 12 or over is legally presumed to have such capacity.

3. What factors are to be taken into account when assessing capacity?

To demonstrate capacity individuals should be able to:

- understand in simple language (with the use of communication aids, if appropriate) what is to be disclosed and why it is being disclosed
- understand the main benefits of disclosure
- understand, in broad terms, the consequences of disclosure
- retain the information long enough to use it and weigh it in the balance in order to arrive at a decision
- communicate the decision (by any means)
- make a free choice (ie free from undue pressure).

4. Determining 'best interests'

All decisions taken on behalf of someone who lacks capacity must be taken in their best interests. A best interests judgement is not an attempt to determine what the patient would have wanted. It is as objective a test as possible of what would be in the patient's actual best interests, taking into account all relevant factors. A number of factors should be addressed including:

- the patient's own wishes (where these can be ascertained)
- where there is more than one option, which option is least restrictive of the patient's future choices

- the views of the parents, if the patient is a child
- the views of people close to the patient, especially close relatives, partners, carers, welfare attorneys, court-appointed deputies or guardians, about what the patient is likely to see as beneficial.

(See also Card 1: '0-18', 'Children', 'Capacity', 'MCA' and 'Scotland Incapacity'.)

CARD 7

Adults who lack capacity

1. Temporary or permanent mental incapacity

Patients with mental disorders or learning disabilities should not automatically be regarded as lacking the capacity to give or withhold their consent to disclosure of confidential information. Unless unconscious, most people suffering from a mental impairment can make valid decisions about some matters that affect them. An individual's mental capacity must be judged in relation to the particular decision being made. If therefore a patient has the requisite capacity, disclosure of information to relatives or third parties requires patient consent. One of the most difficult dilemmas for health professionals occurs where the extent of the patient's mental capacity is in doubt. In such cases health professionals must assess the information which is available from the patient's health record and from third parties. They should attempt to discuss with patients their needs and preferences as well as assess their ability to understand their condition and prognosis. If there is still doubt about a patient's competence to give or withhold consent, health professionals should seek a second opinion.

2. Relatives, carers and friends

If a patient lacks capacity, health professionals may need to share information with relatives, friends or carers to enable them to assess the patient's best interests. Where a patient is seriously ill and lacks

capacity, it would be unreasonable always to refuse to provide any information to those close to the patient on the basis that the patient has not given explicit consent. This does not, however, mean that all information should be routinely shared, and where the information is sensitive, a judgement will be needed about how much information the patient is likely to want to be shared, and with whom. Where there is evidence that the patient did not want information shared, this must be respected.

3. Next of kin

Although widely used, the phrase 'next of kin' has no legal definition or status. If a person is nominated by a patient as next of kin and given authority to discuss the patient's condition, such a person may provide valuable information about the patient's wishes to staff caring for the patient. However, the nominated person cannot give or withhold consent to the sharing of information about the patient and has no rights of access to the patient's medical records. The patient may nominate anyone as next of kin – spouse, partner, family member or friend. In the absence of such a nomination, no-one can claim to be next of kin.

4. Proxy decision-makers

In England and Wales, the Mental Capacity Act 2005 allows people over 18 years of age who have capacity to appoint a welfare attorney to make health and personal welfare decisions once capacity is lost. The Court of Protection may also appoint a deputy to make these decisions. Where a patient lacks capacity and has no relatives or

friends to be consulted, the Mental Capacity Act requires an Independent Mental Capacity Advocate (IMCA) to be appointed and consulted about all decisions about 'serious medical treatment', or place of residence. An attorney or deputy can also be appointed to make decisions relating to the management of property and financial affairs. In the case of health information, health professionals may only disclose information on the basis of the patient's best interests. While it will be necessary for attorneys, deputies and IMCAs to have some information to enable them to act or make decisions on behalf of the patient, that does not mean that they will always need to have access to the whole of the patient's records, but only what is necessary to deal with the issue in question. Where there is no attorney, deputy or IMCA, information should only be disclosed in the patient's best interests.

In Scotland the Adults with Incapacity (Scotland) Act 2000 allows people over the age of 16 who have capacity to appoint a welfare attorney to make health and personal welfare decisions once capacity is lost. The Court of Session may also appoint a deputy to make these decisions. An attorney or deputy can also be appointed to make decisions relating to the management of property and financial affairs. In the case of health information, health professionals may only disclose information when it is of benefit to the patient. While it will be necessary for attorneys and deputies to have some information to enable them to act or make decisions on behalf of the patient, that does not mean that they will always need to

have access to the whole of all the patient's records, only what is necessary to deal with the issue in question. Where there is no attorney or deputy, information should only be disclosed where it is of benefit to the patient.

In Northern Ireland, there is no mental capacity legislation. Information should therefore only be disclosed in accordance with the common law and in the patient's best interests.

5. Abuse and neglect

Where health professionals have concerns about a patient lacking capacity who may be at risk of abuse or neglect, it is essential that these concerns are acted upon and information is given promptly to an appropriate person or statutory body, in order to prevent further harm. Where there is any doubt as to whether disclosure is considered to be in the patient's best interests, it is recommended that the health professional discusses the matter on an anonymised basis with a senior colleague, the Caldicott guardian, their professional body or defence organisation. Health professionals must ensure that their concerns and the actions they have taken or intend to take, including any discussion with the patient, colleagues or professionals in other agencies, are clearly recorded in the patient's medical records.

(See also Card 6 on Assessment of Capacity and Determining 'Best Interests' and Card 10 Public Interest and Card 1: 'Capacity', 'MCA' and 'Scotland Incapacity'.)

CARD 8

Children and young people

1. Competent children

There is no presumption of capacity for people under 16 in England, Wales and Northern Ireland and those under that age must demonstrate they have sufficient understanding of what is proposed. However, children who are aged 12 or over are generally expected to have to have capacity to give or withhold their consent to the release of information. In Scotland, anyone aged 12 or over is legally presumed to have such capacity. Younger children may also have sufficient capacity. When assessing a child's capacity it is important to explain the issues in a way that is suitable for their age. If the child is competent to understand what is involved in the proposed treatment, the health professional should, unless there are convincing reasons to the contrary, for instance abuse is suspected, respect the child's wishes if they do not want parents or guardians to know. However, every reasonable effort must be made to persuade the child to involve parents or guardians particularly for important or life-changing decisions.

2. Children who lack capacity

The duty of confidentiality owed to a child who lacks capacity is the same as that owed to any other person. Occasionally, young people seek medical treatment, for example, contraception, but are judged to lack the capacity to give consent. An explicit request by a child that information should

not be disclosed to parents or guardians, or indeed to any third party, must be respected save in the most exceptional circumstances, for example, where it puts the child at risk of significant harm, in which case disclosure may take place in the 'public interest' without consent. Therefore, even where the health professional considers a child to be too immature to consent to the treatment requested, confidentiality should still be respected concerning the consultation, unless there are very convincing reasons to the contrary. Where a health professional decides to disclose information to a third party against a child's wishes, the child should generally be told before the information is disclosed. The discussion with the child and the reasons for disclosure should also be documented in the child's record.

3. Parental responsibility

Anyone with parental responsibility can give or withhold consent to the release of information where the child lacks capacity. Not all parents have parental responsibility. In relation to children born after 1 December 2003 (England and Wales), 15 April 2002 (Northern Ireland) and 4 May 2006 (Scotland), both of a child's biological parents have parental responsibility if they are registered on a child's birth certificate. In relation to children born before these dates, a child's biological father will only automatically acquire parental responsibility if the parents were married at the time of the child's birth or at some time thereafter. If the parents have never been married, only the mother automatically has parental responsibility, but the father may acquire that status by order or agreement. Neither

parent loses parental responsibility on divorce. Parents who do not have parental responsibility nonetheless play an essential role in determining best interests and may have a right, under the Human Rights Act, to participate in the decision-making process.

Where the child has been formally adopted, the adoptive parents are the child's legal parents and automatically acquire parental responsibility. Where the child has been born as a result of assisted reproduction, there are rules under the Human Fertilisation and Embryology Act 1990 that determine the child's legal parentage. In some circumstances people other than parents acquire parental responsibility, for example by the appointment of a guardian or on the order of a court. A local authority acquires parental responsibility (shared with the parents) while the child is the subject of a care or supervision order. In some circumstances parental responsibility can be delegated to other carers such as grandparents and childminders. If there is doubt about whether the person giving or withholding consent has parental responsibility, legal advice should be sought.

Where an individual who has parental responsibility refuses to share relevant information with other health professionals or agencies and the health professional considers that it is not in the best interests of the child, (for example, it puts the child at risk of significant harm), disclosure may take place in the public interest without consent.

4. Safeguarding children

Where health professionals have concerns about a child who may be at risk of abuse or neglect, it is essential that these concerns are acted upon and information is given promptly to an appropriate person or statutory body, in order to prevent further harm. The best interests of the child or children involved must guide decision-making at all times. Knowing what to do when patients do not want confidential information disclosed, despite this being the best way to ensure that they do not suffer harm or abuse, is very difficult for health professionals. Health professionals should not make promises to the child about confidentiality that they may not be able to keep but, as in the case of any patient, trust is best maintained if disclosure is not made without prior discussion between the health professional and the child, unless to do so would expose the child or others to an increased risk of serious harm.

Where there is any doubt as to whether disclosure is in the child's best interests, it is recommended that the health professional discusses the matter anonymously with an experienced colleague, the Caldicott guardian, their professional body or defence body. Health professionals must ensure that their concerns, and the actions they have taken, or intend to take, including any discussion with the child, colleagues or professionals in other agencies, are clearly recorded in the child's medical record. Health professionals may be involved in case reviews for which the child's records may need to be disclosed, but care should be taken not to disclose the notes of other family members without consent unless it can be justified in the public interest.

(See also Card 6 on Assessment of Capacity and Determining 'Best Interests' and Card 10 on Public Interest and Card 1: '0-18', 'Children', 'Capacity' and 'MET'.)

CARD 9

Legal and statutory disclosures

1. Disclosure required by statute

Health professionals are required by law to disclose certain information, regardless of patient consent. Health professionals must be aware of their obligations to disclose in these circumstances as well as to ensure that they do not disclose more information than is necessary. Where such a statutory requirement exists, patients' consent to disclosure is not necessary. Patients have no right to refuse but they should be generally aware of the disclosure and that it is to a secure authority. Examples of statutory disclosures include:

- Public Health (Control of Disease) Act 1984 and Public Health (Infectious Diseases) Regulations 1988 – a health professional must notify local authorities of the identity, sex and address of any person suspected of having a notifiable disease, including food poisoning
- Abortion Regulations 1991 – a doctor carrying out a termination of pregnancy must notify the Chief Medical Officer, giving a reference number and the date of birth and postcode of the woman concerned
- Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1985 – deaths, major injuries and accidents resulting in more than three days off work, certain diseases and dangerous occurrences must be reported

- Road Traffic Act 1988 – health professionals must provide to the police, on request, any information which may identify a driver alleged to have committed a traffic offence
- Terrorism Act 2000 – all citizens, including health professionals, must inform police as soon as possible of any information that may help to prevent an act of terrorism, or help in apprehending or prosecuting a terrorist
- The Information Sharing Index (England) Regulations 2007 (ContactPoint) – health professionals must provide basic identifying information to the local authority for every child up to the age of 18.

2. Disclosure to the police, social services and partner organisations

Some statutes permit, rather than require, disclosure. Examples include the Data Protection Act 1998, the Crime and Disorder Act 1998 and the Children Act 1989 which permit disclosure to other organisations, such as the police, local authorities, social services, schools, Multi-Agency Protection Panels and government bodies. In such cases, health professionals may only disclose information when the patient has given consent or there is an overriding public interest. If health professionals have any doubts about whether the disclosure is a statutory obligation, they should ask the person or body applying for the information to specify under which legislation it is sought. (See also Card 10 on Public Interest and Card 1: 'DH Code', 'GMC', 'MET', 'NI Confidentiality' and 'Scotland Confidentiality'.)

3. Disclosure to solicitors

Health records that are required for legal proceedings are usually obtained via the Data Protection Act 1998 or Access to Health Records Act 1990. Health professionals releasing information to lawyers acting for their patients should ensure that they have the patient's written consent to disclosure and, where there is any doubt, confirm that the patient understands the nature and extent of the information disclosed. In practice, most solicitors will provide the patient's signed consent when requesting confidential information. If a solicitor acting for someone else seeks information about a patient, their consent to the release of the information must be obtained. Should the patient refuse, the solicitor may apply for a court order requiring disclosure of the information. (See also Card 1: 'Access' and 'IC'.)

4. Disclosure to courts, tribunals and regulatory bodies

The courts, including the coroner's courts, some tribunals, and bodies appointed to hold inquiries such as the General Medical Council, have legal powers to require disclosure, without the patient's consent, of information that may be relevant to matters within their jurisdiction. Applications for court orders must be served on patients who, if they object to the disclosure of the information, must be given an opportunity to make representations to the court. However, often applications are served on health care organisations when they should be served on patients. In these circumstances the patient should be informed of the application so they can make their representations

to court if they object. Where a court order is served health professionals are justified in disclosing information when they believe on reasonable grounds that information falls within this category, and should disclose only as much information as is requested. Failure to comply with a court order to release records may be an offence, but health professionals should object to the judge or presiding officer if they believe that the records contain information that should not be disclosed, for example, because it relates to third parties unconnected with the proceedings. Patients should be informed of disclosures ordered by a court.

5. Statutory restrictions on disclosure

Health professionals are required by law to restrict the disclosure of some specific types of information. For example:

- The Gender Recognition Act 2004 allows transsexual people who have taken decisive steps to live fully and permanently in their acquired gender to apply for legal recognition of that gender. The Act makes it an offence to disclose 'protected information' when that information is acquired in an official capacity. It defines 'protected information' as information about a person's application to the Gender Recognition Panel for gender recognition and a person's gender history after that person has changed gender under the Act. At the time of writing, Department of Health guidance for health care professionals regarding the Act, and specifically how this type of patient information should be recorded, stored and shared is awaited

- The NHS (Venereal Diseases) Regulations 1974 (currently being reviewed by the Department of Health) and the NHS Trusts and PCTs (Sexually Transmitted Diseases) Directions 2000 provide that any information capable of identifying an individual who is examined or treated for any sexually transmitted disease including HIV shall not be disclosed, other than to a medical practitioner in connection with the treatment of the individual or for the prevention of the spread of the disease
- The Human Fertilisation and Embryology Act 1990 protects the confidentiality of the information kept by clinics and the Human Fertilisation and Embryology Authority (HFEA). Information can only be viewed by the clinic licence-holder and by staff or members of the HFEA (plus, in certain circumstances, the Registrar General or a court). Disclosure of information which identifies the patient to another party without the patient's prior consent is a criminal offence.

CARD 10

Public interest

1. General principles

In the absence of patient consent, a legal obligation or anonymisation, any decision as to whether identifiable information is to be shared with third parties must be made on a case by case basis and must be justifiable in the 'public interest'. Public interest is the general welfare and rights of the public that are to be recognised, protected and advanced. Disclosures in the public interest based on the common law are made where disclosure is essential to prevent a serious and imminent threat to public health, national security, the life of the individual or a third party or to prevent or detect serious crime. The GMC also advises that a disclosure without consent can be justified in the public interest to enable medical research. Ultimately, the public interest can only be determined by the courts. However, when considering disclosing information to protect the public interest, health professionals must:

- consider how the benefits of making the disclosure balance against the harms associated with breaching the patient's confidentiality both to the individual clinical relationship and to maintaining public trust in a confidential service
- assess the urgency of the need for disclosure
- persuade the patient to disclose voluntarily
- inform the patient before making the disclosure and seek his or her consent, unless to do so would increase the risk of harm or inhibit effective investigation

- disclose the information promptly to the appropriate body
- reveal only the minimum information necessary to achieve the objective
- seek assurance that the information will be used only for the purpose for which it is disclosed
- document the steps taken to seek or obtain consent, and the reasons for disclosing the information without consent
- be able to justify the decision; and
- document both the extent of and grounds for the disclosure.

Health professionals should be aware that they risk criticism, and even legal liability, if they fail to take action to avoid serious harm. Advisory bodies, such as the BMA, cannot tell health professionals whether or not to disclose information in a particular case, but can provide general guidance about the categories of cases in which decisions to disclose may be justifiable (see below). Guidance should be sought from their Caldicott guardian, professional body or defence body where there is any doubt as to whether disclosure should take place in the public interest.

2. Research

In the past, professional guidance has not viewed medical research as a justifiable reason for a 'public interest' disclosure without consent. Rather, research has been categorised exclusively as a secondary use of data which, aside from disclosures which are covered by law, requires either consent or anonymisation prior to disclosure. (See Card 13: Secondary Uses of Patient information). New GMC

guidance advises that doctors can now disclose identifiable information without consent for research purposes if it is in the public interest.

The GMC guidance states that doctors can disclose identifiable information without consent for research purposes in the public interest if:

- it is necessary to use identifiable information; or
- it is not practicable to anonymise the information and, in either case not practicable to seek consent.

The GMC advises that a number of factors must be taken in to account in any consideration as to whether the research justifies a breach of confidentiality in the public interest:

- the nature of the information must be considered
- the use that will be made of it
- how many people will have access to it
- the security arrangements to protect further disclosure
- the advice of an independent expert advisor, such as a Caldicott Guardian, should be sought
- the potential for harm or distress to patients.

When faced with requests for access to identifiable data from researchers health professionals must assess each case on its individual merits. These decisions are complex and it may be extremely difficult to make a judgement as to when the public interest can or cannot constitute a legitimate disclosure for research. Health professionals are under no obligation to disclose information and should seek further advice from the GMC if there is doubt as to whether the

research is in the public interest. The BMA is of the view that unless health professionals are confident they can make a reasonable assessment as to whether the research is in the public interest a cautious approach should be adopted. Reasons for any disclosure should be documented.

3. Serious crime and national security

There is no legal definition as to what constitutes a 'serious crime'. In the Police and Criminal Evidence Act 1984 a 'serious arrestable offence' is an offence that has caused or may cause:

- serious harm to the security of the state or to public order
- serious interference with the administration of justice or with the investigation of an offence
- death
- serious injury; or
- substantial financial gain or serious loss.

This includes crimes such as murder, manslaughter, rape, treason, kidnapping and abuse of children or other vulnerable people. Serious harm to the security of the state or to public order and serious fraud will also fall into this category. In contrast, theft, minor fraud or damage to property where loss or damage is less substantial would generally not warrant breach of confidence.

4. Public safety

A common example of what can be categorised as public safety occurs in connection with the assessment of patients with, for example, diabetes, epilepsy, defective eyesight, hypoglycaemia or serious cardiac conditions who have been advised

by health professionals to discontinue driving, but who nevertheless continue. The DVLA should be informed if anybody is thought to be at risk.

Issues of public safety may similarly arise in circumstances where an individual who legitimately possesses firearms is thought by health professionals to be a risk because of drug or alcohol addiction or a medical condition such as depression. The police should be informed if anybody is thought to be at risk.

5. Health

When a person has a medical condition that puts others at risk, for example, infection from a serious communicable disease such as HIV, doctors must discuss with the patient how to minimise the risk to others. If patients refuse to modify their behaviour or inform others, doctors are advised by the GMC that they may breach confidentiality and inform a known sexual contact. The same considerations apply to circumstances where the potential disclosure relates to a health professional who poses a threat to the health of patients or colleagues because of illness or addiction.

(See also Card 1: 'GMC', 'DH Code',' MET', NI Confidentiality' and 'Scotland Confidentiality'.)

CARD 11

Deceased patients

1. Are deceased patients owed a duty of confidentiality?

The ethical obligation to respect a patient's confidentiality extends beyond death. The Information Tribunal I England and Wales has also held that a duty of confidence attaches to the medical records of the deceased under section 41 of the Freedom of Information Act. The Freedom of Information Act in Scotland contains an exemption to the disclosure of deceased patients' records. However, this duty of confidentiality needs to be balanced with other considerations, such as the interests of justice and of people close to the deceased person. Health professionals should therefore counsel their patients about the possibility of disclosure after death and solicit views about disclosure where it is obvious that there may be some sensitivity. Such discussions should be noted in the records.

2. Are there any rights of access to a deceased patient's records?

Statutory rights of access are contained within the Access to Health Records Act 1990 and the Access to Health Records (Northern Ireland) Order 1993. Unless the patient requested confidentiality whilst alive, a personal representative or anyone who may have a claim arising out of a patient's death has a right of access to information directly relevant to the claim. Disclosure may take place unless it may cause

'serious harm' to an individual, or if it relates to a third party other than a health professional. Prior to disclosure, advice should be sought from the health professional who last treated the patient. If this health professional is not available, a suitably qualified and experienced health professional must advise. (See also Card 1: 'Access'.)

3. Are relatives entitled to information about the deceased's last illness?

Whilst there is no legal entitlement other than the limited circumstances covered under the Access to Health Records legislation, health professionals have always had discretion to disclose information to a deceased person's relatives or others when there is a clear justification. A common example is when the family requests details of the terminal illness because of an anxiety that the patient might have been misdiagnosed or there might have been negligence. Disclosure in such cases is likely to be what the deceased person would have wanted and may also be in the interests of justice. Refusal to disclose in the absence of some evidence that this was the deceased patient's known wish exacerbates suspicion and can result in unnecessary litigation. In other cases, the balance of benefit to be gained by the disclosure to the family, for example of a hereditary or infectious condition, may outweigh the obligation of confidentiality to the deceased.

CARD 12

Serious communicable diseases

1. Legal restrictions on disclosure

Serious communicable diseases such as HIV remain stigmatised health conditions and many patients regard information about them as particularly sensitive and private. In addition to the common law duty of confidence and the Data Protection Act, there is specific legislation covering the disclosure of information about serious communicable diseases. The legislation, which is currently being reviewed by the Department of Health, is the NHS (Venereal Diseases) Regulations 1974 and the NHS Trusts and PCTs (Sexually Transmitted Diseases) Directions 2000. These provide that any information capable of identifying an individual who is examined or treated for any sexually transmitted disease, including HIV, shall not be disclosed other than to a medical practitioner in connection with the treatment of the individual or for the prevention of the spread of the disease.

2. Can information be disclosed to close sexual contacts?

When a patient has a medical condition that puts others at risk health professionals must discuss with the patient how to minimise that risk. In the case of serious communicable diseases such as HIV, health professionals should discuss with the patient the need to inform sexual partners, and the options for safe sex. Every effort should be made to persuade patients to agree to the information being shared

voluntarily. Patients should also be advised that if they refuse to share the information, the health professional may be obliged to do so. Exceptionally, if patients refuse to modify their behaviour or inform others, doctors are advised by the GMC that they may breach confidentiality and inform a close sexual contact of the patient. Wherever possible, patients should always be told before this step is taken. The GMC advises that doctors should not disclose information to others without patient consent, for example, relatives who have not been and are not at risk of infection. (See also Card 10 on Public Interest and Card 1: 'GMC' and 'MET'.)

3. Can information be disclosed where a health care worker has suffered a needlestick injury or other occupational exposure to blood or bodily fluids?

The use of universal precautions should be enough to protect health care workers from infection, thereby making disclosure unnecessary to prevent 'serious harm'. However, there will be occasions where, for example, despite all reasonable precautions a health professional suffers a needlestick injury and the patient is known by the treating doctor to have a blood-borne virus, such as HIV. If the patient is competent, consent should be sought to disclose information. Where the patient lacks capacity to consent, disclosure may only take place if it is in the best interests of the patient. In the BMA's view it is difficult to envisage how disclosure could be in the patient's best interests and legal advice should be sought on a case-by-case basis. (See also Card 6 on Assessment of Capacity and Determining 'Best Interests' and Card 1: 'Capacity', 'Scotland Incapacity', 'MCA', 'GMC' and 'MET'.)

CARD 13

Secondary uses of patient information

1. What are secondary uses?

Health professionals may receive requests for disclosure of patient information from those not directly involved in the patient's care. Such secondary use of patient information falls into three broad categories:

- use within the NHS for administration, planning, audit, commissioning and payment by results
- use by agencies commissioned by the NHS to carry out such roles on its behalf
- use where identifiable information goes beyond health care provision in the NHS to include research and education.

2. When can information be disclosed for secondary uses?

Patient data may be disclosed to an appropriate and secure authority and used for secondary purposes if:

- they have been effectively anonymised or pseudonymised
- they are required by law
- the patient has given explicit consent
- the health professional is satisfied, in some limited circumstances, that the patient is aware of the use and has not objected to it and so has effectively provided implied consent
- disclosure is authorised by ECC under S251 of the NHS Act 2006 or advice has been sought from the Scottish Government Health Directorates or the Department of Health, Social Services and Public Safety in Northern Ireland

- the health professional is satisfied that the legal and professional criteria for disclosure without consent in the 'public interest' have been met and has sought advice from the Caldicott guardian, professional body or defence organisation in the case of any doubt.

In the absence of patient consent, anonymised data should be used for any secondary purpose where it is practicable to do so. Some secondary uses of patient data are for social purposes unconnected with the provision of health care, eg for insurance or employment purposes. Such disclosure requires explicit patient consent.

(See also Card 1: 'SU' and 'ECC'.)

CARD 14

Uses of information for non-medical purposes

1. Spiritual care

Spiritual care is provided by a range of spiritual advisers. Hospital chaplains can provide vital support and care to people in hospital. Some patients are happy for information about their religious affiliation to be passed to the chaplain, who may then arrange spiritual care in accordance with their wishes. In the case of a competent patient, information about affiliation and clinical information about the patient's health and care should not be passed on without the patient's consent. When patient's lack the capacity to give consent, for example because they are unconscious, those close to the patient should be consulted prior to disclosure of information to explore the patient's wishes, feelings and beliefs. (See also Card 1: 'Chaplaincy' and 'MET'.)

2. Complaints

When a patient initiates a complaint, it is unlikely to be practicable for an investigation to take place without access to the relevant parts of the health record. The use of identifiable information is therefore necessary and appropriate. However, patients should be made aware of who will see information about them, and the safeguards that are in place to minimise any risks to confidentiality. Guidance on maintaining confidentiality in the NHS complaints procedures is available from the health departments. Sometimes patients involve their MP

or other elected representative in the complaints process and where the MP states in writing that they have the patient's consent for disclosure this may usually be accepted without further reference to the patient. However, only information relevant to the complaint should be disclosed and the patient should be copied into the response. Patients are also entitled to authorise relatives or carers to act on their behalf and health professionals who are asked to disclose information in these circumstances must be satisfied that the patient has given valid consent to the disclosure. (See also Card 1: 'DH Code' and ' MET'.)

3. Employers, government departments and insurance companies

When third parties such as insurers or employers ask for information, doctors must have written consent from the patient or a person properly authorised to act on the patient's behalf. The original consent form, or a copy, should be provided by the third party. An electronic copy of the signed form is sufficient, provided that the third party can satisfy the doctor that there are robust mechanisms in place to ensure that the form has not been tampered with in any way. In the case of government departments such as the Benefits Agency, the GMC advises doctors that they may accept written assurances from an officer of a government department that the patient has given written consent to disclosure. In other cases information should not be provided unless evidence is produced. (See also Card 1: 'GMC' and 'MET'.)

CARD 15

Dual responsibilities

1. What are dual responsibilities?

All doctors have multiple professional loyalties, such as those to colleagues, health service employers, and society at large. This card concerns situations in which there is a third party to whom the doctor has potentially conflicting contractual responsibilities, or a court for which a doctor is acting as a witness. Circumstances in which dual obligations arise include:

- doctors providing medical reports for third parties, such as the immigration service, employers, insurers and the courts
- doctors who are employed by third parties, such as occupational physicians, doctors in the armed forces, doctors employed by the benefits agency to assess claims and sports doctors employed by, for example, professional football clubs
- doctors whose jobs do not focus on individual patients, such as doctors in the media or those with business interests.

2. General principles

The following principles should inform doctors' actions with respect to confidentiality where they have dual obligations:

- doctors acting for a third party must ensure that the patient understands that fact, and its implications

- doctors have a duty of confidentiality, and information should not normally be disclosed without the patient's knowledge and consent
- doctors appointed and paid for by a third party still have a duty of care to the patient whom they advise, examine or treat, and must abide by professional guidelines on ethics and law.

Some examples of doctors with dual responsibilities and how these impact on their duty of confidentiality are listed below. There is specific guidance available for doctors working in some specialist areas. For example, the Faculty of Occupational Medicine has produced ethics guidance that covers the issue of confidentiality.

3. Occupational health physicians

Occupational health doctors have the same duties of confidentiality as other doctors. The fact that a doctor is a salaried employee gives no other employee of that company any right of access to medical records or to the details of examination findings. With the employee's consent, the employer may be advised of any relevant information relating to a specific matter on a strictly need to know basis, the significance of which the employee clearly understands.

The guidelines issued by the Faculty of Occupational Medicine state that it is normally appropriate to give employers the outcome of a health assessment, for example a report of being 'fit' or 'unfit' for work, but the clinical details cannot be disclosed unless the individual gives consent.

4. Doctors working in custodial settings

Doctors working in custodial settings should be aware that all detainees have rights of confidentiality but in some cases these are limited and disclosure may be required by statute or by a court. The general principles of confidentiality and disclosure in the public interest also apply.

5. Doctors in the armed forces

Doctors with the armed forces have the same duty of confidentiality as other doctors and disclosure of personal health information should take place with the consent of the patient. The general principles of disclosure in the public interest nevertheless apply and information may have to be disclosed to the commanding officer without the consent of the patient, for example, when the health of the patient puts the health, security and safety of the unit or the patient at risk.

(See also Card 10 on Public Interest and Card 1: 'GMC' and 'MEC'.)

CARD 16

Useful names and addresses

British Medical Association
Medical Ethics Department, BMA House,
Tavistock Square, London WC1H 9JP.
Tel: 020 7383 6286
Fax: 020 7383 6233
Web: www.bma.org.uk/ethics

Connecting for Health
Princes Exchange, Princes Square,
Leeds, West Yorkshire LS1 4HY.
Tel: 0113 397 3333 or 0113 397 3335
Web: www.connectingforhealth.nhs.uk

Department of Health
Wellington House,
133-55 Waterloo Road, London SE1 8UG.
Tel: 020 7972 2000
Web: www.doh.gov.uk

Ethics and Confidentiality Committee
National Information Governance Board Office
Floor 7, New Kings Beam House,
22 Upper Ground, London SE1 9BW
Tel: 020 7633 7052
Web: www.nigb.nhs.uk/ecc

Faculty of Occupational Medicine
of the Royal College of Physicians
6 St Andrew's Place, Regent's Park,
London NW1 4LB.
Tel: 020 7317 5890
Fax: 020 7317 5899
Web: www.facoccmed.ac.uk/index.jsp

Faculty of Pharmaceutical Medicine
1 St Andrew's Place, Regent's Park,
London NW1 4LB.
Tel: 020 7224 0343
Fax: 020 7224 5381
Web: www.fpm.org.uk

General Medical Council
Regents Place, 350 Euston Road,
London, NW1 3JN.
Tel: 020 7189 5404
Fax: 020 7189 5401
Web: www.gmc-uk.org

Health Professions Council, Park House
184 Kennington Park Road,
London SE11 4BU.
Tel: 020 7582 0866
Fax: 020 7820 9684
Web: www.hpc-uk.org

Medical and Dental Defence Union
of Scotland
Mackintosh House, 120 Blythswood Street,
Glasgow G2 4EA.
Tel: 0141 221 5858
Fax: 0141 228 1208
Web: www.mddus.com

Medical Defence Union
230 Blackfriars Road, London SE1 8PG.
Tel: 020 7202 1500
Fax: 020 7202 1666
Web: www.the-mdu.com

Medical Foundation for AIDS
and Sexual Health
BMA House, Tavistock Square, London WC1H 9JP.
Tel: 020 7383 6345
Fax: 020 7388 2544
Web: www.medfash.org.uk

Medical Protection Society
33 Cavendish Square, London W1G 0PS.
Tel: 0845 605 4000
Fax: 020 7399 1301
Web: www.mps.org.uk

National Information Governance Board
for Health and Social Care
NIGB secretariat, Floor 7, New Kings Beam House,
22 Upper Ground, London, SE1 9BW.
Tel: 020 7 633 7206
Web: www.connectingforhealth.nhs.uk/nigb

Northern Ireland Department of Health, Social
Services and Public Safety
Castle Buildings, Stormont, Belfast BT4 3SJ.
Tel: 028 90520500
Web: www.dhsspsni.gov.uk

Nursing and Midwifery Council
23 Portland Place, London W1B 1PZ.
Tel: 020 7637 7181
Fax: 020 7436 2924
Web: www.nmc-uk.org

Office of the Public Guardian and the Court of Protection (England and Wales)
Archway Tower, 2 Junction Road,
London, N19 5SZ.
Tel: 0845 330 2900
Fax: 020 7664 7705
Web: www.publicguardian.gov.uk

Office of the Public Guardian (Scotland)
Hadrian House, Callendar Business Park,
Callendar, Road, Falkirk, FK1 1XR.
Tel: 01324 678300
Fax: 01234 67830
Web: www.publicguardian-scotland.gov.uk

Royal College of General Practitioners
14 Princes Gate, Hyde Park, London SW7 1PU.
Tel: 020 7581 3232
Fax: 020 7225 3047
Web: www.rcgp.org.uk

Royal College of Nursing
20 Cavendish Square, London W1M 0AB.
Tel: 020 7409 3333
Fax: 020 7647 3435
Web: www.rcn.org.uk

Royal College of Obstetricians and Gynaecologists
27 Sussex Place, London NW1 4RG.
Tel: 020 7772 6200
Fax: 020 7723 0575
Web: www.rcog.org.uk

Royal College of Ophthalmologists
17 Cornwall Terrace, London NW1 4QW.
Tel: 020 7935 0702
Fax: 020 7935 9838
Web: www.rcophth.ac.uk

Royal College of Paediatrics and Child Health
50 Hallam Street, London W1N 6DE.
Tel: 020 7307 5600
Fax: 020 7307 5601
Web: www.rcpch.ac.uk

Royal College of Pathologists
2 Carlton House Terrace, London SW1Y 5AF.
Tel: 020 7451 6700
Fax: 020 7451 6701
Web: www.rcpath.org

Royal College of Physicians
11 St Andrew's Place, London NW1 4LE.
Tel: 020 7935 1174
Fax: 020 7487 5218
Web: www.rcplondon.ac.uk

Royal College of Physicians and Surgeons of Glasgow
232-42 St Vincent Street, Glasgow G2 5RJ.
Tel: 0141 221 6072
Fax: 0141 221 1804
Web: www.rcpsglasg.ac.uk

Royal College of Physicians of Edinburgh
9 Queen Street, Edinburgh EH2 1JQ.
Tel: 0131 225 7324
Fax: 0131 220 3939
Web: www.rcpe.ac.uk

Royal College of Psychiatrists
17 Belgrave Square, London SW1X 8PG.
Tel: 020 7235 2351
Fax: 020 7245 1231
Web: www.rcpsych.ac.uk

Royal College of Radiologists
38 Portland Place, London W1N 4JQ.
Tel: 020 7636 4432
Fax: 020 7323 3100
Web: www.rcr.ac.uk

Royal College of Surgeons of Edinburgh
Nicolson Street, Edinburgh EH8 9DW.
Tel: 0131 527 1600
Fax: 0131 557 6406
Web: www.rcsed.ac.uk

Royal College of Surgeons of England
35-43 Lincoln's Inn Fields, London WC2A 3PN.
Tel: 020 7405 3474
Fax: 020 7831 9438
Web: www.rcseng.ac.uk

Scottish Government Health Directorate
St Andrew's House, Regent Road,
Edinburgh EH1 3DG.
Tel: 0131 556 8400
Fax: 0131 244 8240
Web: www.sehd.scot.nhs.uk/

For further information about these guidelines, BMA members may contact:

the BMA on 0300 123 123 3 or

British Medical Association
Department of Medical Ethics, BMA House
Tavistock Square, London WC1H 9JP.
Tel: 020 7383 6286
Fax: 020 7383 6233
Email: ethics@bma.org.uk

Non-members may contact:

British Medical Association
Public Affairs Department, BMA House
Tavistock Square, London WC1H 9JP.
Tel: 020 7387 4499
Fax: 020 7383 6400
Email: info.public@bma.org.uk