Ethics Department

Guidance on secondary uses of patient information

What are “secondary uses”?

Balancing competing rights

What data are confidential?

Sources of confidentiality rights and protections

Circumstances permitting disclosure of identifiable data

- Disclosures required by law
- Consent to disclosure
- Disclosures in the public interest

April 2007

BMA

What are "secondary uses"?

Patient health information is collected primarily to provide care for individual patients and it can be used freely for this purpose subject to the constraints set out in the Department of Health code on Confidentiality.[1] However, secondary uses of patient information are more likely to be subject to a higher standard where disclosure is concerned in particular, for example, ancillary purposes such as health care planning, clinical audit and administration. No breach of patient confidentiality occurs if the secondary use is carried out by healthcare professionals who already have access to the information in their role of providing care; for example, where audit or planning is undertaken within the health team. Nevertheless, patients should be made aware that this is taking place. In this guidance, we focus on disclosure outside the team and consider three broad categories of secondary use:

- Use within the NHS for administration, planning, audit;
- 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.

Safeguards are essential for disclosure but arguably the more distant the data use from the direct provision of patient care, the more robust the safeguards should be as the more unlikely it is patients will be aware of it, or the uses to which such data will be put, unless explicitly asked about it. As is discussed in detail below, it is good practice always to use anonymised data for any secondary purpose where it is practicable to do so and to raise patient awareness about such usage.

Some secondary uses of patient data are for social purposes unconnected with provision of health care, such as disclosure of patient information for insurance or employment purposes. Such disclosure requires explicit patient consent and is covered by other guidance from the BMA.

Balancing competing rights

Patients should be able to expect that information about their health which has been given in confidence, will be kept private unless there is a compelling reason why it should not. Trust in the doctor-patient relationship depends on reciprocal honesty. Frank and open exchange between health professionals and patients is the ideal, and patients need to feel that their privacy will be respected before they can enter into such an exchange. One person's claim to privacy, however, could infringe on the competing claims of others who, for example, as patients wish to benefit from useful research or to avoid communicable diseases and who as tax-payers, wish to support an efficient and effective health service. Where a person's claim to privacy has little or no effect on others, then there is a clear ethical duty of confidence. What is less clear is the extent to which individual rights to privacy should give way to the health benefits of society as a whole. This tension may sometimes be decided by law and sometimes by debate. The consequence of this blend of competing interests is that doctors must ensure that patient identifiable information is processed fairly and confidentiality is protected. In return, it is fair and lawful to share information from patients, provided that they are involved in decisions about the release of their identifiable information to third parties and wherever possible anonymised data are used.

What data are confidential?

Traditionally, professional ethical standards have required that anything doctors learned about a patient in the course of their professional duties was confidential. Nowadays, this is also reflected in legal rules. Confidentiality 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 a patient 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.

Sources of confidentiality rights and protections

The use of information about individual patients is governed by:

- Data Protection Act 1998 (the DPA) – the DPA came into force in March 2000. Its purpose is to protect the right of the individual to privacy with respect to the processing of personal data. It governs when and in what circumstances personal data may be shared with others but even when data sharing is justifiable, the Act only *permits* and does not *require* the release of information. The DPA requires organisations to process fairly and lawfully any information which might enable a patient to be identified. The DPA's requirement is that all processing must be "fair", "lawful" and also "necessary". The provision of patient-identifiable information is permissible where it is a necessary function of the operation of the NHS. Fair processing therefore must entail the doctor doing all that is reasonable in the circumstances to ensure that patients are aware of what information about them is being processed and when it is being processed, and in certain circumstances where feasible those patients should be contacted directly for their consent (see NHS Code of Confidentiality). Furthermore, the DPA requires organisations that wish to process identifying information to use the minimum of information necessary and to retain it only for as long as is needed for the purpose for which it was originally collected.

- Human Rights Act 1998 (the HRA) – a right to "respect for private and family life" is guaranteed in article 8 of the 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 confidentiality may be breached where other significant interests prevail.

- Health and Social Care Act 2001 - in England and Wales, Section 60 of the Health and Social Care Act 2001 gives the Secretary of State power to make regulations permitting the disclosure of identifiable information without consent in certain very tightly defined and unusual circumstances which are set out on the website.[2] Health Professionals can apply to the Patient Information Advisory Group (PIAG), an independent public body which advises the Secretary of State for England and Wales about the lawful basis for disclosure of patient identifiable information.

- 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. ("Public interest" disclosure is discussed further below.)

- Professional Standards – all healthcare professionals must maintain the standards of confidentiality laid down by their professional body, such as the General Medical Council, or risk complaint for professional misconduct which may result in a reprimand or removal from the register.

- 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. These include the Caldicott Guardian Manual (2006), the Department of Health Confidentiality NHS Code of Practice (2003) and the Scottish Executive NHS Code of Practice on Protecting Patient Confidentiality (2003).

It is important to note that the legal position on confidentiality is complex. 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. For example 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 (see below). Doctors who are uncertain about the application of the law in a particular case should seek legal advice. Doctors must also ensure that their actions comply with the guidance issued by the General Medical Council.

Anonymisation

A principle that underpins the BMA's views on confidentiality and access to information is that 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. Health professionals must take reasonable steps to anonymise data to this extent, and if necessary, take technical advice about anonymisation before releasing data. Although there should be safeguards to prevent inappropriate use or abuse of even anonymous information, in general the Association believes that it is not ethically necessary to seek consent for its use. This is also the position in law. The Court of Appeal, in a decision about prescribing data, confirmed that there was no legal duty of confidentiality when data were anonymous.[3] The BMA therefore advocates anonymisation as a solution to the difficulties of gaining consent for the sharing of personal data with third parties. Nevertheless, it is important to note that whilst the Data Protection Act does not restrict the use of data that do not identify patients, patients should generally know when it is intended that their information will be anonymised for a range of appropriate purposes.

Example

GPs may be asked to disclose data about patients for health planning purposes and anonymised information is usually sufficient. For example in order to anticipate and plan for the numbers of patients likely to require emergency hospital admission over a winter period, analysts may need anonymised data from a practice about the numbers of patients with certain conditions. It is good practice for doctors to take steps to ensure patients are generally aware that anonymised data are used to improve health services even though patients' agreement to non-identifiable use is not required.

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 references to information 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. It must however still meet the " fair processing" requirements of the DPA. 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.

Circumstances permitting disclosure of identifiable data

All identifiable health information health professionals acquire in a professional capacity is subject to the duty of confidentiality and so should not be disclosed. There are three broad exceptions:

- where the law requires disclosure
- where there is appropriate consent
- where there is an overriding public interest.

1. Disclosures required by law

Health professionals are required by law to disclose certain information, regardless of patient consent. The principal subjects of statute and regulations are potential dangers to society from serious communicable diseases and in the interests of order and justice. Doctors 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

Under public health legislation, doctors must notify local authorities of the identity, sex and address of any person having a notifiable disease, including food poisoning. [4] Deaths, major injuries and accidents resulting in more than three days off work, certain diseases and dangerous occurrences must be reported under health and safety legislation.[5] 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.[6]

2. Consent to disclosure

Consent to disclosure may be explicit or implied. It may also be consent to disclosure 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. There will be a number of standard purposes for which the personal data of all patients entering a hospital or registering with a GP will be processed. It is good practice to provide information to all patients about these standard uses at the outset of care rather than have to repeatedly pose the same question. They include disclosures of personal data for purposes such as audit, Post-Payment Verification (PPV) and Quality and Outcomes Framework (QOF). Implied or explicit patient consent is acceptable as long as patients are aware of the potential disclosure and the choice of opting out.

Explicit consent

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

The GMC provides the following guidance:

> " where clinical audit is to be undertaken by another organisation, information should be anonymised wherever that is practicable. In any case where it is not practicable to anonymise data, or anonymised data will not fulfil the requirements of the audit, express consent must be obtained before identifiable data is disclosed".[7]

The GMC further states:

> " express consent is usually needed before the disclosure of identifiable information for purposes such as research, epidemiology, financial audit or administration (but see page 5). When seeking express consent to disclosure you must make sure that patients are given enough information on which to base their decision, the reason for the disclosure and the likely consequences of the disclosure. You should also explain how much information will be disclosed and to whom it will be given. If the patient withholds consent, or consent cannot be obtained, disclosures may be made only where they are required by law or can be justified in the public interest. Where the purpose is covered by a regulation made under s60 of the Health and Social Care Act 2001, disclosures may also be made without patient's consent. You should make a record of the patient's decision, and whether and why you have disclosed information."[8]

Example of explicit consent

GPs are often asked by researchers to help recruit patients with a specific condition to participate in a research project. Normal procedure would be for the GP to send letters enclosing information provided by the researcher which outline the details of the project to a selection of patients with the condition, inviting them to respond if they are willing for their names to go forward. Those who do respond positively effectively provide explicit consent to the disclosure of their names to the researcher.

Implied consent

As well as explicit consent, patient agreement can also be implied, signalled by the behaviour of an informed patient. Implied consent is not a lesser form of consent but it only has validity if the patient *genuinely* knows what is proposed and knows that he or she has a choice about participating. If not, it is no consent at all and some other justification will be needed for its disclosure. The concept of implied consent arose initially in the context of consent to treatment rather than consent to disclosure. It is easy to verify implied consent to treatment, if patients – having been informed of the reasons for a particular procedure – indicate by their actions that they agree to it. With implied consent to disclosure, verification is harder and doctors should take reasonable steps to ensure that this is obtained. Problems arise as it is often difficult to know with any certainty if patients really know either about the proposed sharing of information or their rights to opt out of it. **It should be noted that the more sensitive and detailed the data the more likely it is that express consent will be required e.g. sexual health information.**

The BMA, Department of Health[9] and the General Medical Council[10] have long accepted that, unless the patient objects, implied consent is appropriate for the sharing of information among those directly contributing to the diagnosis, care or treatment of that patient. When identifiable information is needed for secondary purposes such as research, teaching, financial audit or to plan or run services, and anonymisation is not practicable the view has been, as set out in the GMC's advice quoted above, that competent patients should usually be asked to give explicit consent. It must be emphasised that with either explicit or implied consent, patients have the right to withhold or withdraw consent to information they provide being disclosed to a third party. This means they need to know that their identifiable information might be sent to other people unless they object. Failing to provide sufficient information about the project or an opportunity to object could invalidate either kind of consent.

Providing information for explicit and implied consent

Doctors must take reasonable steps to ensure that the patient's consent to disclosure for secondary purposes – whether implied or explicit – is valid and much depends on the information provided. Explicit consent remains best

practice and should be the norm where possible as it provides patients with opportunities to ask questions and actively share in decisions about the uses of their information. There are some circumstances where, even though explicit consent would be best practice, implied consent is acceptable in the interests of the health of the population and future health needs and improvements. Nevertheless, it is only acceptable if patients have been clearly informed about the uses to which their data may be put.

Explicit consent or refusal is relatively straightforward but relying on implied consent can be problematic. The Information Commissioner states that the provision of "fair processing information" solely by means of a poster in the surgery or waiting room or by a notice in the local paper is **unlikely** to be sufficient to meet the requirements of the Data Protection Act since not all patients will see or be able to understand such information.[11]

GMC advice

The GMC advises:

> " You should record financial or other administrative data separately from clinical information. When asked to disclose information you should provide it in an anonymised form, or obtain express consent. However, some current systems may prevent data being anonymised, or express consent being sought or acted on. You must draw attention to systems which prevent you from following best practice, and recommend change. Until that is achieved you should obtain implied consent, by ensuring patients are aware of disclosures made for financial, administrative and other purposes, and of their right to object, or be satisfied that such information has been provided. You should provide further information about the nature and purpose of the disclosures, if this is requested. You should do your best to act on any objections to disclosures…..Additionally in England and Wales, you can seek support for such disclosures without consent under s60 of the Health and Social care Act 2001".[12]

Advice from the Information Commissioner

Methods by which fair processing information may be provided include.[13]

- posters plus a standard information leaflet,
- information provided face to face in the course of a consultation,
- information included with an appointment letter from a hospital or clinic,
- information in a letter sent to each patient's home.

Clearly a combination of methods provide greater security that patients have understood. The effort involved in providing this information may be minimised by integrating the process with existing procedures, such as mentioning data use in the course of face to face discussions between patients and practice staff. Most GP practices already provide information to patients by means of posters and leaflets about how the practice operates and could incorporate the fair processing information in these. Wherever possible, patients should have a variety of sources of information, not only on paper but also by methods such as web, fax, e-mail and by telephone.

Example of implied consent

A GP practice does not have the necessary systems which would enable it to anonymise the significant amount of patient identifiable information required by a PCT for the purposes of PPV visits and nor for the same reason is it practicable to obtain explicit consent from each individual patient. Patients attending the GP practice are given an information leaflet about the need to release information for financial and administrative purposes in order to support the wider functioning of the NHS, including the management of health care services. Receptionists and other practice staff draw their attention to this and ensure that the information is understood as well as ensuring that posters are seen inviting patients to raise any questions. All the patient information should make it clear their option of refusing for their own information to be used. As long as the doctors in the practice are satisfied that they have done all that is reasonable in their particular circumstances to ensure that all those attending the surgery have been made aware that their information will be used for this purpose, this could be an instance where implied consent is relied upon in relation to those patients (i.e. for those who did go to the surgery).

3. Disclosures in the public interest

In the absence of patient consent 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". Traditionally, 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. This is how the BMA has generally interpreted the concept of public interest disclosure. Confidentiality is seen to be too important a principle to be sacrificed for vague goals or indefinable harm, but should give way where there is some "serious" threat to people. The General Medical Council also provides guidance to doctors on what they must consider prior to making a disclosure in the public interest.

GMC advice on disclosures in the public interest

> "Personal information may be disclosed in the public interest, without patient's consent, and in exceptional circumstances where patients have withheld consent, **where the benefits to an individual or to society of the disclosure outweigh the public and patient's interest in keeping the information confidential.** (emphasis added) In all cases where you consider disclosing information without consent from the patient, you must weigh the possible harm (both to the patient and the overall trust between doctors and patients) against the benefits which are likely to arise from the release of information…. Ultimately, the "public interest" can be determined only by the courts; but the GMC may also require you to justify your actions if it receives a complaint about the disclosure of identifiable information without a patient's consent."[14]

Although in the past, the BMA has tended to espouse a fairly narrow definition of public interest, it recognises that in the context of secondary use of information, public interest must be a balance between individuals' and society's rights and claims to confidentiality and the rights and claims of the whole of society to better health and to

protection against threats to ill health. Any disclosure of identifiable information must be proportionate to the anticipated benefit and subject to good governance rules. To make such an evaluation requires consideration of:

- the degree of disclosure and the expected benefits for society
- the degree of intrusiveness for the patient
- the level of public awareness and acceptance of the disclosure

As the GMC's advice makes clear, what constitutes the public interest in any case is ultimately a matter for the law although in extreme cases where non-disclosure represents a serious threat to the health or welfare of individuals, e.g. child protection, it will almost inevitably be in the public interest to share information appropriately with third parties. However, in all other cases, unless it is absolutely clear that the disclosure is in the "public interest" doctors would be well advised to adopt a cautious approach and seek the advice of the GMC.

Where there is no other legal basis for the secondary use of the information that can identify patients, then health professionals can apply to the Patient Information Advisory Group (PIAG) under section 60 of the Health and Social Care Act. PIAG is an independent public body which advises the Secretary of State for England and Wales about the lawful basis for information that may identify patients to be released to third parties such as medical researchers, NHS bodies and other health bodies without first seeking patient consent. Health professionals have to make a strong argument that their work is in the public interest, needs identifiers and that it would not be feasible or appropriate to anonymise or get patient consent. Examples of where PIAG has granted or refused applications for disclosure of patient identifiable information without consent are contained in its annual report. In Scotland and Northern Ireland there is no equivalent body and it is therefore recommended that health professionals in these circumstances should seek advice from the Scottish Executive Health Department and the Department of Health, Social Services and Public Safety in Northern Ireland or directly with the GMC.

Conclusion

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

- they have been effectively anonymised
- they are identifiable but required by law
- the patient has given explicit consent
- the health professional is satisfied 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 PIAG under S60 of the Health and Social Care Act or advice has been sought from the Scottish Executive Health Department 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 taken advice from the GMC in the case of any doubt.

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

*ask*BMA on 0870 60 60 828 **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 6403
Email: info.public@bma.org.uk

References

1 Department of Health. *Confidentiality: NHS Code Of Practice*, November 2003

2 www.advisorybodies.doh.gov.uk/piag

3 R v Department of Health (Respondent), ex parte Source Informatics Ltd (Appellant) and (1) Association Of The British Pharmaceutical Industry (2) General Medical Council (3) Medical Research Council (4) National Pharmaceutical Association Ltd (Interveners). [2001] 1 All ER 786.

4 Public Health (Control of Diseases) Act 1984.

5 Reporting of Injuries, Diseases, and Dangerous Occurrences Regulations 1985 (S1 1985 No. 2023 as amended).

6 Department of Health. *Guidance note for completing the abortion notification form HSA4*: DOH 2002.

7 General Medical Council. *Confidentiality: protecting and providing information.* London: GMC, 2004: para 15

8 General Medical Council. *Confidentiality: protecting and providing information.* Op cit: para *16*

9 Department of Health. *Confidentiality : NHS Code of Practice*, Op cit: para 15

10 General Medical Council. *Confidentiality: protecting and providing information.* Op cit: para 10

11 Data Protection Act 1998 and Post Payment Verification – Guidance from Health Compliance Department of the Information Commissioner

12 General Medical Council. *Confidentiality: protecting and providing information.* Frequently Asked Questions: Q9

13 Data Protection Act 1998 and Post Payment Verification – Guidance from Health Compliance Department of the Information Commissioner . Op cit

14 General Medical Council. Confidentiality: *protecting and providing information*. Op cit: paras 22 and 26