Confidentiality

NHS Code of Practice

November 2003

Confidentiality

NHS Code of Practice

November 2003

READER INFORMATION

Policy HR/Workforce Management Planning Clinical	Estates Performance IM & T Finance Partnership Working
Document Purpose	Best Practice Guidance
ROCR Ref:	**Gateway Ref:** 1656
Title	NHS Confidentiality Code of Practice
Author	DH/IPU/Patient Confidentiality
Publication date	ASAP
Target Audience	Caldicott Guardians and Data Protection Officers
Circulation list	PCT CEs, NHS Trusts CEs, Care Trusts CEs, Directors of HR, Communications Leads, WDC CEs, Voluntary Organisations
Description	Purpose is to provide guidance to the NHS and NHS related organisations on patient information confidentiality issues. BMA, GMC and OIC have endorsed the document. This will help send a consistent message across the Service on confidentiality and issues around the processing of patient information.
Cross Ref	HSG(96)18/LASSL(96)5 – The Protection and Use of Patient Information
Superseded Doc	HSG(96)18/LASSL(96)5 – The Protection and Use of Patient Information
Action required	Ministerial approval to publish
Timing	N/A
Contact Details	David Martin Department of Health Confidentiality Unit, IPU Quarry House Leeds david.martin@doh.gsi.gov.uk 0113 254 6267
For recipient use	

Contents

Foreword

The 'Confidentiality: NHS Code of Practice' has been published by the Department of Health following a major public consultation in 2002/2003. The consultation included patients, carers and citizens; the NHS; other health care providers; professional bodies and regulators. The guidance was drafted and delivered by a working group made up of key representatives from these areas.

Endorsements from the Information Commissioner, General Medical Council, British Medical Association and Medical Research Council can be found on the Department of Health's Confidentiality website http://www.doh.gov.uk/ipu/confiden

Introduction and Glossary

1. This document is a guide to required practice for those who work within or under contract to NHS organisations concerning confidentiality and patients' consent to the use of their health records. It replaces previous guidance, HSG (96)18/LASSL (96) 5 – The Protection and Use of Patient Information and is a key component of emerging information governance arrangements for the NHS.

2. For the purposes of this document, the term 'staff' is used as a convenience to refer to all those to whom this code of practice should apply. Whilst directed at NHS staff, the Code is also relevant to any one working in and around health. This includes private and voluntary sector staff.

3. This document

   a. introduces the concept of confidentiality;

   b. describes what a confidential service should look like;

   c. provides a high level description of the main legal requirements;

   d. recommends a generic decision support tool for sharing/disclosing information;

   e. lists examples of particular information disclosure scenarios.

4. A summary of the key confidentiality issues can be gained by reading the main body of the document (pages 1-12), while the supporting Annexes provide detailed advice and guidance on the delivery of a confidential service.

5. This is an evolving document because the standards and practice covered continue to change. Where appropriate, it is supplemented by additional guidance on the Department of Health web-site at www.doh.gov.uk/ipu/confiden.

6. All parts of the NHS need to establish working practices that effectively deliver the patient confidentiality that is required by law, ethics and policy. The objective must be continuous improvement.

7. NHS managers need to be able to demonstrate active progress in enabling staff to conform to these standards, identifying resource requirements and related areas of organisation or system change. Performance assessment and management arrangements in support of information governance in the NHS facilitate and drive forward the required change. Those responsible for monitoring NHS performance, e.g. strategic health authorities and the Commission for Health Audit and Inspection (CHAI) play a key role in ensuring effective systems are in place.

8. The NHS are provided with support to deliver change through the:

   a. Information Governance Toolkit which will manage and maintain up-to-date confidentiality policy and guidance and, more generally;

   b. Information Governance teams within the Information Policy Unit of the Department of Health and the NHS Information Authority.

Figure 1

The NHS is committed to the delivery of a first class confidential service. This means ensuring that all patient information is processed fairly, lawfully and as transparently as possible so that the public:

- understand the reasons for processing personal information;
- give their consent for the disclosure and use of their personal information;
- gain trust in the way the NHS handles information and;
- understand their rights to access information held about them.

Glossary of Terms

Patient identifiable information	Key identifiable information includes: • patient's name, address, full post code, date of birth; • pictures, photographs, videos, audio-tapes or other images of patients; • NHS number and local patient identifiable codes; • anything else that may be used to identify a patient directly or indirectly. For example, rare diseases, drug treatments or statistical analyses which have very small numbers within a small population may allow individuals to be identified.
Anonymised Information	This is information which does not identify an individual directly, and which cannot reasonably be used to determine identity. Anonymisation requires the removal of name, address, full post code and any other detail or combination of details that might support identification.
Pseudonymised Information	This is like anonymised information in that in the possession of the holder it cannot reasonably be used by the holder to identify an individual. However it differs in that the original provider of the information may retain a means of identifying individuals. This will often be achieved by attaching codes or other unique references to information so that the data will only be identifiable to those who have access to the key or index. Pseudonymisation allows information about the same individual to be linked in a way that true anonymisation does not.
Clinical Audit	The evaluation of clinical performance against standards or through comparative analysis, with the aim of informing the management of services. This should be distinguished from studies that aim to derive, scientifically confirm and publish generalisable knowledge. The first is an essential component of modern healthcare provision, whilst the latter is research and is not encompassed within the definition of clinical audit in this document.
Explicit or Express Consent	This means articulated patient agreement. The terms are interchangeable and relate to a clear and voluntary indication of preference or choice, usually given orally or in writing and freely given in circumstances where the available options and the consequences have been made clear.
Implied consent	This means patient agreement that has been signalled by behaviour of an informed patient.

Disclosure	This is the divulging or provision of access to data.
Healthcare Purposes	These include all activities that directly contribute to the diagnosis, care and treatment of an individual and the audit/assurance of the quality of the healthcare provided. They do not include research, teaching, financial audit and other management activities.
Information Sharing Protocols	Documented rules and procedures for the disclosure and use of patient information, which specifically relate to security, confidentiality and data destruction, between two or more organisations or agencies.
Medical Purposes	As defined in the Data Protection Act 1998, medical purposes include but are wider than healthcare purposes. They include preventative medicine, medical research, financial audit and management of healthcare services. The Health and Social Care Act 2001 explicitly broadened the definition to include social care.
Public Interest	Exceptional circumstances that justify overruling the right of an individual to confidentiality in order to serve a broader societal interest. Decisions about the public interest are complex and must take account of both the potential harm that disclosure may cause and the interest of society in the continued provision of confidential health services.
Social Care	Social care is the support provided for vulnerable people, whether children or adults, including those with disabilities and sensory impairments. It excludes "pure" health care (hospitals) and community care (e.g. district nurses), but may include items such as respite care. There is therefore, no clear demarcation line between health and social care. Social care also covers services provided by others where these are commissioned by CSSRs (Councils with Social Service Responsibilities).

Confidentiality

What is confidential patient information?

9. A duty of confidence arises when one person discloses information to another (e.g. patient to clinician) in circumstances where it is reasonable to expect that the information will be held in confidence. It –

   a. is a legal obligation that is derived from case law;

   b. is a requirement established within professional codes of conduct; and

   c. must be included within NHS employment contracts as a specific requirement linked to disciplinary procedures.

10. Patients entrust us with, or allow us to gather, sensitive information relating to their health and other matters as part of their seeking treatment. They do so in confidence and they have the legitimate expectation that staff will respect their privacy and act appropriately. In some circumstances patients may lack the competence to extend this trust, or may be unconscious, but this does not diminish the duty of confidence. It is essential, if the legal requirements are to be met and the trust of patients is to be retained, that the NHS provides, and is seen to provide, a confidential service. What this entails is described in more detail in subsequent sections of this document, but a key guiding principle is that a patient's health records are made by the health service to support that patient's healthcare.

11. One consequence of this is that information that can identify individual patients, must not be used or disclosed for purposes other than healthcare without the individual's explicit consent, some other legal basis, or where there is a robust public interest or legal justification to do so. In contrast, anonymised information is not confidential and may be used with relatively few constraints.

Figure 2

Patient information is generally held under legal and ethical obligations of confidentiality. Information provided in confidence should not be used or disclosed in a form that might identify a patient without his or her consent. There are a number of important exceptions to this rule, described later in this document, but it applies in most circumstances.

Disclosing and using confidential patient information

12. It is extremely important that patients are made aware of information disclosures that must take place in order to provide them with high quality care. In particular, clinical governance and clinical audits, which are wholly proper components of healthcare provision, might not be obvious to patients and should be drawn to their attention. Similarly, whilst patients may understand that information needs to be shared between members of care teams and between different organisations involved in healthcare provision, this may not be the case and the efforts made to inform them should reflect the breadth of the required disclosure. This is particularly important where disclosure extends to non-NHS bodies.

13. Many current uses of confidential patient information do not contribute to or support the healthcare that a patient receives. Very often, these other uses are extremely important and provide benefits to society – e.g. medical research, protecting the health of the public, health service management and financial audit. However, they are not directly associated with the healthcare that patients receive and we cannot assume that patients who seek healthcare are content for their information to be used in these ways. Further details on information disclosure and sharing can be found at Annex B.

Patient consent to disclosing

14. Patients generally have the right to object to the use and disclosure of confidential information that identifies them, and need to be made aware of this right. Sometimes, if patients choose to prohibit information being disclosed to other health professionals involved in providing care, it might mean that the care that can be provided is limited and, in extremely rare circumstances, that it is not possible to offer certain treatment options. Patients must be informed if their decisions about disclosure have implications for the provision of care or treatment. Clinicians cannot usually treat patients safely, nor provide continuity of care, without having relevant information about a patient's condition and medical history.

15. Where patients have been informed of:

    a. the use and disclosure of their information associated with their healthcare; and

    b. the choices that they have and the implications of choosing to limit how information may be used or shared;

    then explicit consent is not usually required for information disclosures needed to provide that healthcare. Even so, opportunities to check that patients understand what may happen and are content should be taken. Special attention should be paid to the issues around child consent – see Annex B, paragraphs 9 and 10.

16. Where the purpose is not directly concerned with the healthcare of a patient however, it would be wrong to assume consent. Additional efforts to gain consent are required or alternative approaches that do not rely on identifiable information will need to be developed.

17. There are situations where consent cannot be obtained for the use or disclosure of patient identifiable information, yet the public good of this use outweighs issues of privacy. Section 60 of the Health and Social Care Act 2001 currently provides an interim power to ensure that patient identifiable information, needed to support a range of important work such as clinical audit, record validation and research, can be used without the consent of patients.

Obligations on individuals working in the NHS

18. All staff should meet the standards outlined in this document, as well as their terms of employment (or other engagement agreements). Much of what is required builds on existing best practice. What is needed is to make this explicit and to ensure that everyone strives to meet these standards and improves practice.

19. Clearly staff are constrained from meeting these standards where appropriate organisational systems and processes are not yet in place. In these circumstances the test must be whether they are working within the spirit of this code of practice and are making every reasonable effort to comply.

20. The need for change may apply to many existing systems and processes and it is important that staff know who – perhaps the Caldicott Guardian[1] or information governance lead – should be informed of any specific problems or barriers to change that are noted.

1 A key recommendation of the 1997 Caldicott Report was the establishment of a network of Caldicott Guardians throughout the NHS to oversee access to patient-identifiable information – see www/doh.gov.uk/ipu/confiden for further details.

Providing a Confidential Service

The Confidentiality Model

21. The model outlines the requirements that must be met in order to provide patients with a confidential service. Record holders must inform patients of the intended use of their information, give them the choice to give or withhold their consent as well as protecting their identifiable information from unwarranted disclosures. These processes are inter-linked and should be ongoing to aid the improvement of a confidential service. The four main requirements are:

a. **PROTECT** – look after the patient's information;

b. **INFORM** – ensure that patients are aware of how their information is used;

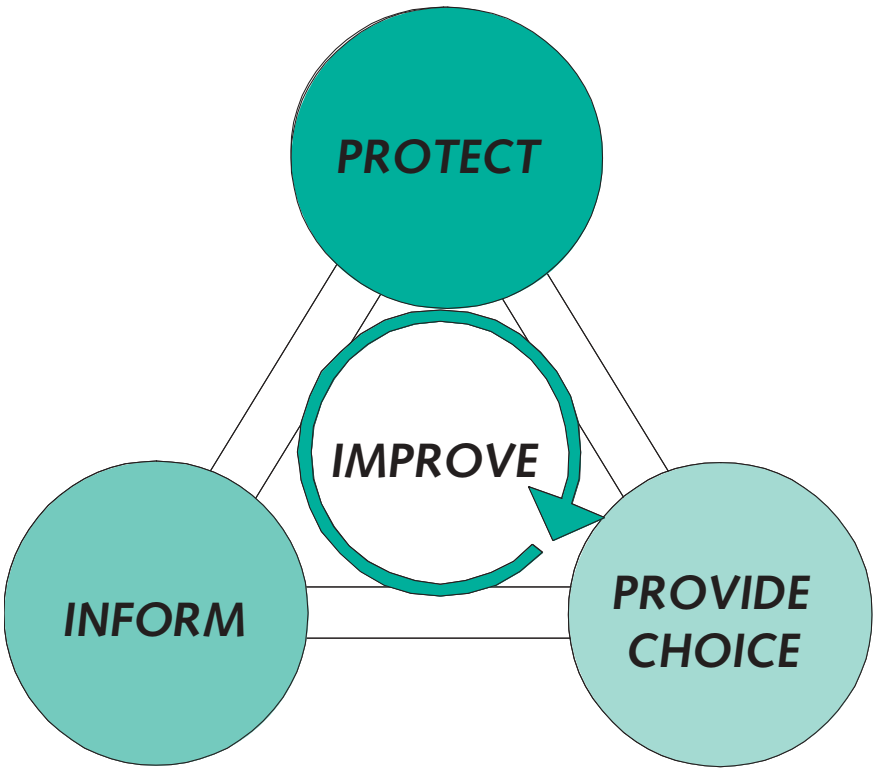
c. **PROVIDE CHOICE** – allow patients to decide whether their information can be disclosed or used in particular ways.

To support these three requirements, there is a fourth:

d. **IMPROVE** – always look for better ways to protect, inform, and provide choice.

These are expanded in the following sections and explored in more detail in Annex A.

Figure 3 – Confidentiality Model



Protect Patient Information

22. Patients' health information and their interests must be protected through a number of measures:

    a. Procedures to ensure that all staff, contractors and volunteers are at all times fully aware of their responsibilities regarding confidentiality;

    b. Recording patient information accurately and consistently;

    c. Keeping patient information private;

    d. Keeping patient information physically secure;

    e. Disclosing and using information with appropriate care.

    See Annex A1 for more detail.

Inform Patients Effectively – No Surprises

23. Patients must be made aware that the information they give may be recorded, may be shared in order to provide them with care, and may be used to support clinical audit and other work to monitor the quality of care provided. Consider whether patients would be surprised to learn that their information was being used in a particular way – if so, then they are not being effectively informed.

24. In order to inform patients properly, staff must:

    a. check where practicable that information leaflets on patient confidentiality and information disclosure have been read and understood. These should be available within each NHS organisation;

    b. make clear to patients when information is recorded or health records are accessed;

    c. make clear to patients when they are or will be disclosing information with others;

    d. check that patients are aware of the choices available to them in respect of how their information may be disclosed and used;

    e. check that patients have no concerns or queries about how their information is disclosed and used;

    f. answer any queries personally or direct the patient to others who can answer their questions or other sources of information;

    g. respect the rights of patients and facilitate them in exercising their right to have access to their health records.

    See Annex A2 for more detail.

Provide Choice to Patients

25. Patients have different needs and values – this must be reflected in the way they are treated, both in terms of their medical condition and the handling of their personal information. What is very sensitive to one person may be casually discussed in public by another – just because something does not appear

to be sensitive does not mean that it is not important to an individual patient in his or her particular circumstances.

26. Staff must:

a. ask patients before using their personal information in ways that do not directly contribute to, or support the delivery of, their care;

b. respect patients' decisions to restrict the disclosure or use of information, except where exceptional circumstances apply;

c. communicate effectively with patients to ensure they understand what the implications may be if they choose to agree to or restrict the disclosure of information.

See Annex A3 for more detail.

Improve Wherever Possible

27. It is not be possible to achieve best practice overnight. Staff must:

a. Be aware of the issues surrounding confidentiality, and seek training or support where uncertain in order to deal with them appropriately.

b. Report possible breaches or risk of breaches.

See Annex A4 for more detail.

Using and Disclosing Confidential Patient Information

28. The disclosure and use of confidential patient information needs to be both lawful and ethical. Whilst law and ethics in this area are largely in step, the law provides a minimum standard that does not always reflect the appropriate ethical standards that the government and the professional regulatory bodies require. For example, the Department of Health and the General Medical Council are in agreement that, whilst there are no clear legal obligations of confidentiality that apply to the deceased, there is an ethical basis for requiring that confidentiality obligations, as outlined in this document, must continue to apply. Further, where the law is unclear, a standard may be set, as a matter of policy, which clearly satisfies the legal requirement and may exceed some interpretations of the law.

Legal Considerations

29. There are a range of statutory provisions that limit or prohibit the use and disclosure of information in specific circumstances and, similarly, a range of statutory provisions that require information to be used or disclosed. The statutory restrictions are described within Annex B. Legal requirements and permissions are continually being added to however, so up to date details can be found on the Department of Health web-site at http://www.doh.gov.uk/ipu/confiden. Generally, however, there are four main areas of law which constrain the use and disclosure of confidential personal health information. These are briefly described below but are covered in more detail within Annex B.

Common Law of Confidentiality

30. This is not codified in an Act of Parliament but built up from case law where practice has been established by individual judgements. The key principle is that information confided should not be used or disclosed further, except as originally understood by the confider, or with their subsequent permission. Whilst judgements have established that confidentiality can be breached 'in the public interest', these have centred on case-by-case consideration of exceptional circumstances. Confidentiality can also be overridden or set aside by legislation.

Data Protection Act 1998 (DPA98)

31. This Act provides a framework that governs the processing of information that identifies living individuals – personal data[2] in Data Protection terms. Processing includes holding, obtaining, recording, using and disclosing of information and the Act applies to all forms of media, including paper and images. It applies to confidential patient information but is far wider in its scope, e.g. it also covers personnel records.

---

2 Personal data is defined under the DPA98 as *'data which relate to a living individual who can be identified – (a) from those data, or (b) from those data and other information which is in the possession of, or likely to be in the possession of, the data controller – and includes any expression of opinion about the individual and any indications of the intentions of the data controller or any other person in respect of the individual'.*

32. The DPA98 imposes constraints on the processing of personal information in relation to living individuals. It identifies eight data protection principles that set out standards for information handling[3]. In the context of confidentiality, the most significant principles are:

- the 1st, which requires processing to be fair and lawful and imposes other restrictions, and;
- the 2nd, which requires personal data to be processed for one or more specified and lawful purposes;
- the 7th, which requires personal data to be protected against unauthorised or unlawful processing and against accidental loss, destruction or damage.

There are a range of DPA98 requirements that are outside the scope of confidentiality and more information can be found at the Information Commissioner's www.informationcommissioner.gov.uk

Human Rights Act 1998 (HRA98)

33. Article 8 of the HRA98 establishes a right to 'respect for private and family life'. This underscores the duty to protect the privacy of individuals and preserve the confidentiality of their health records. Current understanding is that compliance with the Data Protection Act 1998 and the common law of confidentiality should satisfy Human Rights requirements.

34. Legislation generally must also be compatible with HRA98, so any proposal for setting aside obligations of confidentiality through legislation must:

a. pursue a legitimate aim;

b. be considered necessary in a democratic society; and

c. be proportionate to the need.

35. There is also a more general requirement that actions that interfere with the right to respect for private and family life (e.g. disclosing confidential information) must also be justified as being necessary to support legitimate aims and be proportionate to the need.

Administrative Law

36. Administrative law governs the actions of public authorities. According to well-established rules a public authority must possess the power to carry out what it intends to do. If not, its action is *"ultra vires"*, i.e. beyond its lawful powers. It is also necessary that the power be exercised for the purpose for which it was created or be "reasonably incidental" to the defined purpose. It is important that all NHS bodies be aware of the extent and limitations of their powers and act *"intra vires"*.

37. The approach often adopted by Government to address situations where a disclosure of information is prevented by lack of function (the ultra vires rule), is to create, through legislation, new statutory gateways that provide public sector bodies with the appropriate information disclosure function. However, unless such legislation explicitly requires that confidential patient information be disclosed, or provides for common law confidentiality obligations to be set aside, then these obligations must be satisfied prior to information disclosure and use taking place, e.g. by obtaining explicit patient consent.

---

3 For details of the conditions relevant for purposes of the first principle: processing of any personal data and of sensitive personal data, see Schedules 2 and 3 respectively of the Data Protection Act 1998 (Reprinted to incorporate corrections 2003 – pages 52-54). There are also 2 statutory instruments to be aware of: 2000 No.417 The Data Protection (Processing of Sensitive Personal Data) Order 2000, and: 2002 No. 2905 the Data Protection (Processing o/f Sensitive Personal Data (Elected Representatives) Order 2002. Details of both can be found at www.hmso.gov.uk

Key Questions for Confidentiality Decisions

38. A number of key questions have been distilled to ensure that the requirements of law, ethics and policy are adequately addressed when making decisions about the use or disclosure of confidential patient information. These key questions, outlined below, underpin the decision support tool provided at Annex B and the examples of confidentiality decisions provided at Annex C.

If the purpose served by disclosing is not healthcare or another medical purpose, what is the basis in administrative law for disclosing?

Public sector bodies should only do the things that they have been set up to do. Whilst medical purposes are permitted, disclosures to other agencies for other purposes may not be.

Is disclosure either a statutory requirement or required by order of a court?

Although disclosure should be limited to that required and there may be scope to ask the court to amend an order, at the end of the day any disclosure that has either a statutory requirement or court order must be complied with.

Is the disclosure needed to support the provision of healthcare or to assure the quality of that care?

Patients understand that some information about them must be shared in order to provide them with care and treatment, and clinical audit, conducted locally within organisations is also essential if the quality of care is to be sustained and improved. Efforts must be made to provide information, check understanding, reconcile concerns and honour objections. Where this is done there is no need to seek explicit patient consent each time information is shared.[4]

If not healthcare, is the disclosure to support a broader medical purpose?

Preventative medicine, medical research, health service management, epidemiology etc are all medical purposes as defined in law. Whilst these uses of information may not be understood by the majority of patients, they are still important and legitimate pursuits for health service staff and organisations. However, the explicit consent of patients must be sought for information about them to be disclosed for these purposes in an identifiable form unless disclosure is exceptionally justified in the public interest or has temporary support in law under section 60 of the Health & Social Care Act 2001.

Is the use of identifiable and confidential patient information justified by the purpose?

Where the purpose served is not to provide healthcare to a patient and is not to satisfy a legal obligation, disclosure should be tested for appropriateness and necessity, with the aim of minimising the identifiable information disclosed and anonymising information wherever practicable.

Have appropriate steps been taken to inform patients about proposed disclosures?

There is a specific legal obligation to inform patients in general terms, who sees information about them and for what purposes. Where the purpose of providing information is also to seek consent, more detail may be necessary and patients need to be made aware of their rights and how to exert them. See Annex A2 for more detail.

Is the explicit consent of a patient needed for a disclosure to be lawful?

Unless disclosure of identifiable patient information is required by law or the courts, is for a healthcare purpose, can be justified as sufficiently in the public interest to warrant breach of confidence, or is supported by section 60 of the Health & Social Care Act 2001, explicit consent is required.

4 NB: any "other" organisational forms of audit, i.e. across organisations and nationally, require explicit consent.

Annex A – Providing a Confidential Service: Detailed Requirements

A1 Protect Patient Information

Patients' health information and their interests must be protected through a number of measures:

1. Recognising that confidentiality is an obligation for all staff, external contractors, and volunteers.

a. The duty of confidentiality arises out of the common law[5] of confidentiality, professional obligations, and also staff employment contracts (including those for contractors). Breach of confidence, inappropriate use of health records or abuse of computer systems may lead to disciplinary measures, bring into question professional registration and possibly result in legal proceedings. Staff should ensure that they are aware of the requirements and standards of behaviour that apply.

b. Voluntary staff who are not employees, and students are also under obligations of confidentiality, and must sign an agreement indicating their understanding when helping within the NHS.

2. Recording patient information accurately and consistently

Maintaining proper records is vital to patient care (see figure 4). If records are inaccurate, future decisions may be wrong and harm the patient. If information is recorded inconsistently, then records are harder to interpret, resulting in delays and possible errors. The information may be needed not only for the immediate treatment of the patient and the audit of that care, but also to support future research that can lead to better treatments in the future. The practical value of privacy enhancing measures and anonymisation techniques will be undermined if the information they are designed to safeguard is unreliable.

3. Keeping patient information private

This includes aspects such as:

a. Not gossiping.

This is clearly an improper use of confidential information.

b. Taking care when discussing cases in public places.

It may be pertinent to discuss cases with colleagues for professional reasons (to gain advice, or share experience and knowledge), but care must be taken to ensure that others do not overhear these conversations. Generally, there is no need to identify the patient concerned.

5 The rules are extrapolated from the decisions of the courts.

Figure 4 – Record keeping best practice

Patient records should:

be factual, consistent and accurate

- be written as soon as possible after an event has occurred, providing current information on the care and condition of the patient;
- be written clearly, legibly and in such a manner that they cannot be erased;
- be written in such a manner that any alterations or additions are dated, timed and signed in such a way that the original entry can still be read clearly;
- be accurately dated, timed and signed or otherwise identified, with the name of the author being printed alongside the first entry;
- be readable on any photocopies;
- be written, wherever applicable, with the involvement of the patient or carer;
- be clear, unambiguous, (preferably concise) and written in terms that the patient can understand. Abbreviations, if used, should follow common conventions;
- be consecutive;
- (for electronic records) use standard coding techniques and protocols;
- be written so as to be compliant with the Race Relations Act and the Disability Discrimination Act.

Be relevant and useful

- identify problems that have arisen and the action taken to rectify them;
- provide evidence of the care planned, the decisions made, the care delivered and the information shared;
- provide evidence of actions agreed with the patient (including consent to treatment and/or consent to disclose information).

And include

- medical observations: examinations, tests, diagnoses, prognoses, prescriptions and other treatments;
- relevant disclosures by the patient – pertinent to understanding cause or effecting cure/treatment;
- facts presented to the patient;
- correspondence from the patient or other parties.

Patient records should not include

- unnecessary abbreviations or jargon;
- meaningless phrases, irrelevant speculation or offensive subjective statements;
- Irrelevant personal opinions regarding the patient.

4. Keeping patient information physically and electronically secure

This section covers both manual and electronic records. Staff should not leave portable computers, medical notes or files in unattended cars or in easily accessible areas. Ideally, store all files and portable equipment under lock and key when not actually being used. Staff should not normally take patient records home, and where this cannot be avoided, procedures for safeguarding the information effectively should be locally agreed.

Figure 5 – Keeping patient information secure

For all types of records, staff working in offices where records may be seen must:

- Shut/lock doors and cabinets as required.
- Wear building passes/ID if issued.
- Query the status of strangers.
- Know who to tell if anything suspicious or worrying is noted.
- Not tell unauthorised personnel how the security systems operate.
- Not breach security themselves.

Manual records must be:

- Formally booked out from their normal filing system.
- Tracked if transferred, with a note made or sent to the filing location of the transfer.
- Returned to the filing location as soon as possible after use.
- Stored securely within the clinic or office, arranged so that the record can be found easily if needed urgently.
- Stored closed when not in use so that contents are not seen accidentally.
- Inaccessible to members of the public and not left even for short periods where they might be looked at by unauthorised persons.
- Held in secure storage with clear labelling. Protective 'wrappers' indicating sensitivity – though not indicating the reason for sensitivity – and permitted access, and the availability of secure means of destruction, e.g. shredding, are essential.

With electronic records, staff must:

- Always log-out of any computer system or application when work on it is finished.
- Not leave a terminal unattended and logged-in.
- Not share logins with other people. If other staff have need to access records, then appropriate access should be organised for them – this must not be by using others' access identities.
- Not reveal passwords to others.
- Change passwords at regular intervals to prevent anyone else using them.
- Avoid using short passwords[6], or using names or words that are known to be associated with them (e.g. children's or pet's names or birthdays).
- Always clear the screen of a previous patient's information before seeing another.
- Use a password-protected screen-saver to prevent casual viewing of patient information by others.

6 For more detail, please refer to Dr. R.J. Anderson et al. – *The Memorability and Security of Passwords – Some Empirical Results*, http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/tr500.pdf

5. Disclosing information with appropriate care

a. *Follow any established information sharing protocols.*

NHS organisations should have developed, or be in the process of developing, information sharing protocols that set out the standards and procedures that should apply when disclosing confidential patient information with other organisations and agencies. Staff must work within these protocols where they exist, and within the spirit of this code of practice where they are absent.

b. *Identify enquirers, so that information is only shared with the right people.*

Staff should check that any callers, by telephone or in person, are who they say they are. There can be a significant risk of harm to a patient through impersonation by those seeking information improperly. Seek official identification or check identity by calling them back (using an independent source for the phone number). Check also that they have a legitimate right to have access to that information.

c. *Ensure that appropriate standards are applied in respect of e-mails, faxes and surface mail*

Care must be taken, particularly with confidential clinical information, to ensure that the means of transferring it from one location to another are as secure as they can be. Guidance is available on the Department of Health web-site at www.doh.gov.uk/ipu/confiden.

d. *Share the minimum necessary to provide safe care or satisfy other purposes.*

This must clearly be balanced against the need to provide safe care where missing information could be dangerous. It is important to consider how much information is needed before disclosing it. Simply providing the whole medical file is generally needless and inefficient (for both parties), and is likely to constitute a breach of confidence. The Caldicott principles[7] should be followed–

Figure 6 – The Caldicott Principles

i. *Justify the purpose.*

ii. *Don't use patient identifiable information unless it is absolutely necessary.*

iii. *Use the minimum necessary patient identifiable information.*

iv. *Access to patient identifiable information should be on a strict need to know basis.*

v. *Everyone should be aware of their responsibilities.*

vi. *Understand and comply with the law.*

7 Further details are available at http://www.doh.gov.uk/ipu/confiden/index6.htm

A2 Inform Patients Effectively – No Surprises

Patients must be made aware that the information they give may be recorded, may be shared in order to provide them with care, and may be used to support local clinical audit and other work to monitor the quality of care provided. Consider whether patients would be surprised to learn that their information was being used in this way – if so, then they are not being informed correctly.

In order to inform patients properly, staff must themselves be familiar with the content of local patient information leaflets etc, and must:

6. Check that patients have seen the available information leaflets

a. Every NHS organisation should have information leaflets, posters and other materials to support communications about confidentiality and the way that patient information is used and shared.

b. Must incorporate checks within their everyday working practice e.g.

i. Receptionists at clinics or surgeries could ask when patients arrive if they have seen the relevant leaflets, and should offer patients the leaflet if not – this should be supported with encouragement to raise any concerns, perhaps *'Do let me know if you have any queries or would like more information'*.

ii. Clinicians too could check that the patient has had an opportunity to read and understand the leaflets provided – *'Have you read the poster/leaflet on information disclosures and use?'*

7. Make clear to patients when information is recorded or health records are accessed

This may require no more than a comment such as *'Let me note that in your file'*, or *'I am just taking a note of your blood pressure'*, and should occur naturally as part of treating patients properly.

8. Make clear to patients when information is or may be disclosed to others

a. Patients may know little about how the NHS and related agencies e.g. social services, local government and education work – aspects that staff may take for granted. Staff must ensure that patients know when data is disclosed or used more widely. Examples might be:

i. in respect of a referral letter – *'I am writing to the consultant to let them know about your medical history and the abdominal pains you are having'*; or

ii. with electronic records, *'The hospital specialist is able to view your health records to understand your medical history and the tests we have arranged to date before he examines you'*; or

iii. in respect of other agencies – *'I will tell Social Services about your dietary needs to help them arrange Meals on Wheels for you'*.

b. There are certain Acts of Parliament that require disclosure – see www.doh.gov.uk/ipu/confiden. Court orders may also require a disclosure. The amount of information disclosed should always be proportionate to the actual need. Even though the patient cannot prevent this disclosure, they must normally be told that it is taking place or that it has already occurred if this is the case.

9. Check that patients are aware of the choices available in respect of how their information may be used or shared

Patients have the right to choose whether or not to agree to information that they have provided in confidence being used or shared beyond what they understood to be the case when they provided the information. There are exceptions to this, as described in Annex B. Where the information disclosure hasn't yet taken place, they are also entitled to change their mind.

10. Check that patients have no concerns or queries about how their information is used

a. It is important that patients feel free to raise any queries or concerns. In most circumstances it may require no more than a follow-on question to the above: *'Did you understand the leaflet? – Did it make sense to you?'*

b. In other cases, if it is clear that the information being recorded is particularly sensitive to the patient concerned, staff should be explicit about what information is being recorded, and ask the patient directly if he or she is happy with that information being shared.

11. Answer any queries personally or direct patients to others who can answer their questions or other sources of information

a. It is much better for patients if their concerns can be addressed immediately, but, if staff cannot answer the questions properly, they must refer the patient to a better source of information. Most organisations should have arranged back-up contacts for further information e.g. Patient Advisory Liaison (PALs) Officers.

b. In some areas, e.g. GP surgeries or clinics, procedures may have been set up so that patients' queries can be referred to a local designated individual to avoid disrupting the clinical workload.

12. Respect the right of patients to have access to their health records

Patients have a right to see and/or have copies of their health records under the Data Protection Act – see existing guidelines on charges, procedures and exceptions at www.doh.gov.uk/ipu/confiden.

13. Communicate effectively with patients to help them understand

It is important to recognise the different communications needs of particular patients. While some may read NHS leaflets when waiting for treatment, others may be disinclined or unable to do so (perhaps through disability, illiteracy, cultural issues or language difficulties). Difficulty in communicating does not remove the obligation to help people understand.

A3 Provide Choice to Patients

Patients have different needs and values – this must be reflected in the way they are treated, both in terms of their medical condition and the handling of their personal information. What is very sensitive to one person may be casually discussed in public by another – just because something does not appear to be sensitive does not mean that it is not important to an individual patient in his or her particular circumstances. Patients have the right to choose whether or not to accept a form of care and the information disclosure needed to provide that care, and to choose whether or not information that can identify them can be used for non-healthcare purposes.

Although other purposes may generate greater concern, the disclosure of information for healthcare purposes is not normally an issue for the great majority of patients. Even for healthcare however this cannot be taken for granted and patients must be given opportunities to raise objections and concerns. The development of a truly confidential service will maximise patient trust and minimise the number of objections raised. Whilst it is necessary to disclose information about a patient to those staff who are providing or auditing care, it is important to ensure that those who see information have a genuine need to know. Staff must:

14. Ask patients before using their personal information in ways that do not directly contribute to, or support the delivery of their care.

a. Where information about patients is required, but does not satisfy the tests of necessity and appropriateness that must govern the use of identifiable patient information, then it should be anonymised to protect the patient.

b. In all other circumstances efforts must be made to obtain and record consent unless there are statutory grounds for setting confidentiality aside or robust public interest issues.

15. Respect patients' decisions to restrict the disclosure and/or use of information[8]

a. In some cases, it may not be possible to restrict information disclosure without compromising care. This would require careful discussion with the patient, but ultimately the patient's choice must be respected.

b. In the short-term it may not be possible to meet some patients' requests directly though, with some imagination, a compromise arrangement may be possible. This may require discussion about where the patient's concerns really lie as it may be possible to allay those concerns without significant change to the information disclosure arrangements, perhaps by explaining more fully the security arrangements in place, or discussing options in the care process.

c. It is essential that complete records are kept of all care provided and of any restrictions placed on disclosing by patients. When patients impose constraints it is important to demonstrate that neither patient safety, nor clinical responsibility for healthcare provision, has been neglected.

8 Through the advent of Electronic Records and the Integrated Care Delivery System, NHS systems should provide sufficient flexibility to meet all reasonable requests.

16. Explain the implications of disclosing and not disclosing

a. In order to make valid choices, patients must not only know what their options are, but also what the consequences are of making those choices. Explanations must be proportionate to the risks involved and reflect, where possible, the patient's particular circumstances.

b. Where patients insist on restricting how information may be used or shared in ways that compromise the health service's ability to provide them with high quality care, this should be documented within the patient's record. It should be made clear to the patient that they are able to change their mind at a later point.

A4 Improve wherever possible

Although it will not be possible to achieve best practice overnight, NHS organisational confidentiality procedures should be regularly reviewed and the policy in this document adhered to. The NHSIA Information Governance Toolkit will assist the NHS in this. In particular staff must:

17. Be aware of the issues surrounding confidentiality, and seek training or support where uncertain in order to deal with them appropriately

Ignorance is no excuse – so staff must be aware of the basic requirements and where support and further information are available, and encouraged to seek out training and guidance in order to develop confidential services. Staff must work within both the spirit of this code of practice, and within any locally produced guidelines, protocols and procedures, and be able to demonstrate that they are making every reasonable effort to comply with relevant standards.

18. Report possible breaches or risk of breach

a. If staff identify possible breaches or risk of breaches, then they must raise these concerns with their manager or other appropriate colleagues, e.g. the local Information Governance Lead. Staff must be encouraged and supported by management to report organisational systems or procedures that need modification. Staff must be made aware of local procedures for reporting where breaches of confidentiality or abuses of patient data are taking place.

b. There is specific legislation[9] to protect individuals reporting abuses, as well as NHS procedures to support this where necessary (individual NHS organisations will have their own procedures, or independent advice can be obtained from Public Concern at Work (www.pcaw.co.uk)). Professional staff may also choose to contact their professional, regulatory or indemnifying bodies for specific guidance.

9 Public Interest Disclosure Act 1998

Annex B – Confidentiality Decisions[10]

This Annex provides generic guidance where there is a need to disclose information that identifies an individual and that information is held under a legal obligation of confidentiality. The issues to be considered and the appropriate steps to take can be ascertained by working through the model and referenced text.

A range of information disclosure scenarios can be found in Annex C. These reference and illustrate the model provided here and can be used to aid decision-making. They highlight issues relating to particular decisions, e.g. disclosure to NHS managers or to the police. It is hoped that they cover many of the circumstances that staff currently have to deal with. As new issues are identified they will be added to Annex C and updated on line at www.doh.gov.uk/ipu/confiden.

The model is in three parts:

B1 where it is proposed to disclose confidential information in order to provide healthcare.

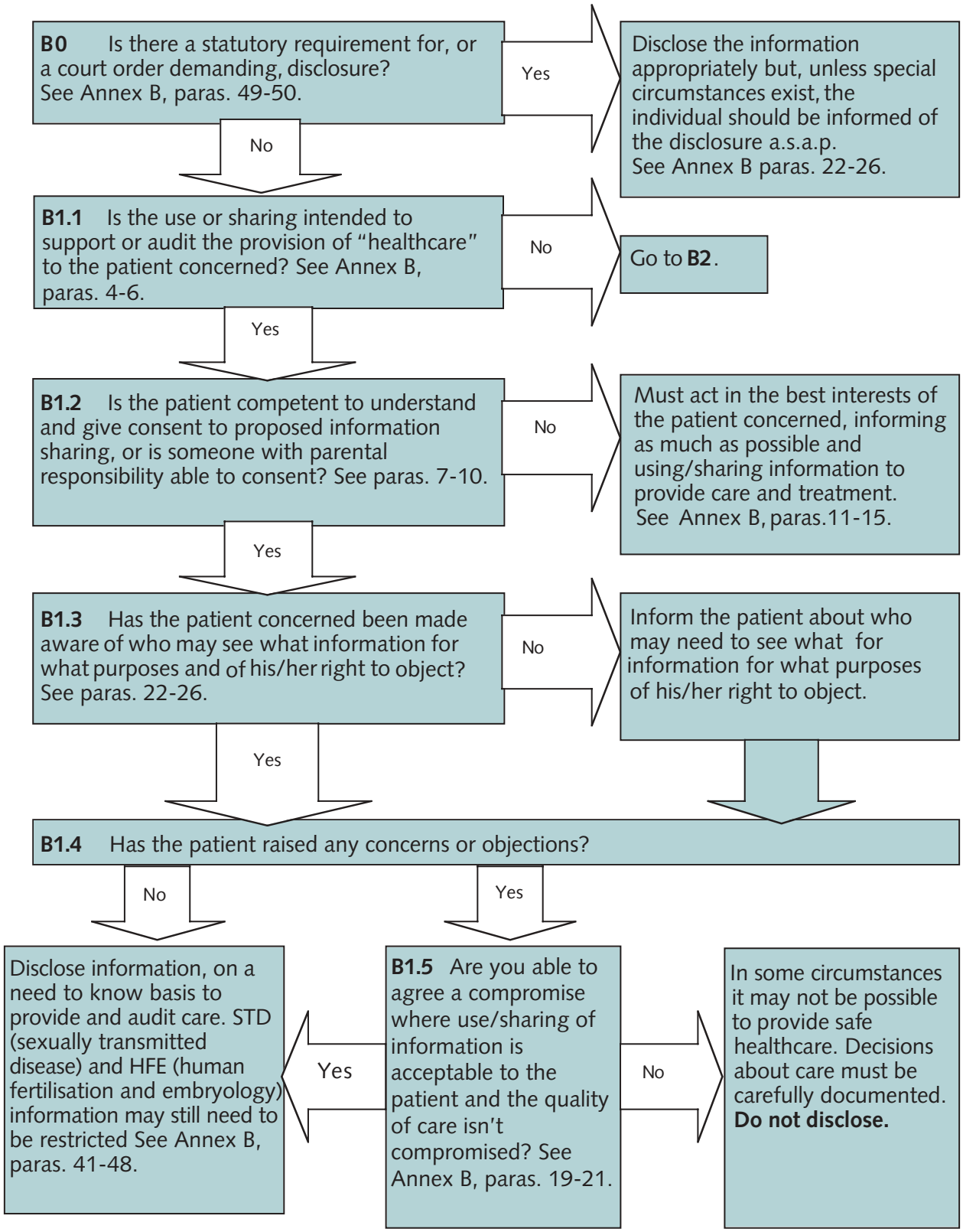
B2 where the purpose isn't healthcare but it is a medical purpose as defined in legislation.

B3 where the purpose is unrelated to healthcare or another medical purpose.

These are important distinctions, in that the legal and ethical requirements differ in each case.

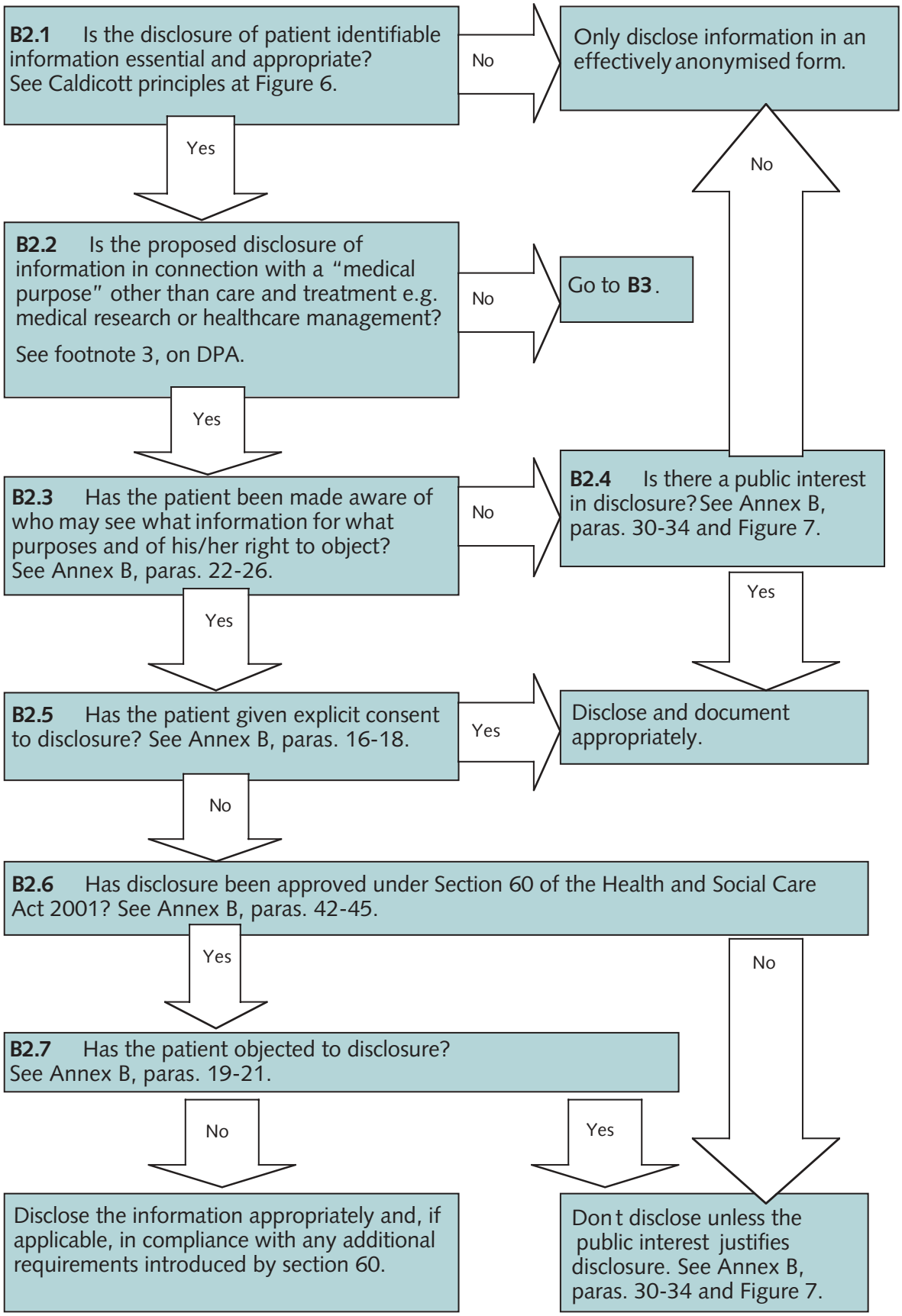
10 It is assumed within this methodology that the member of staff making a confidentiality decision is working within an organisation that may legitimately process health information for healthcare purposes, i.e. that this is a legitimate function of the organisation concerned.

B1: Disclosure Model[11] – where it is proposed to share confidential information in order to provide healthcare

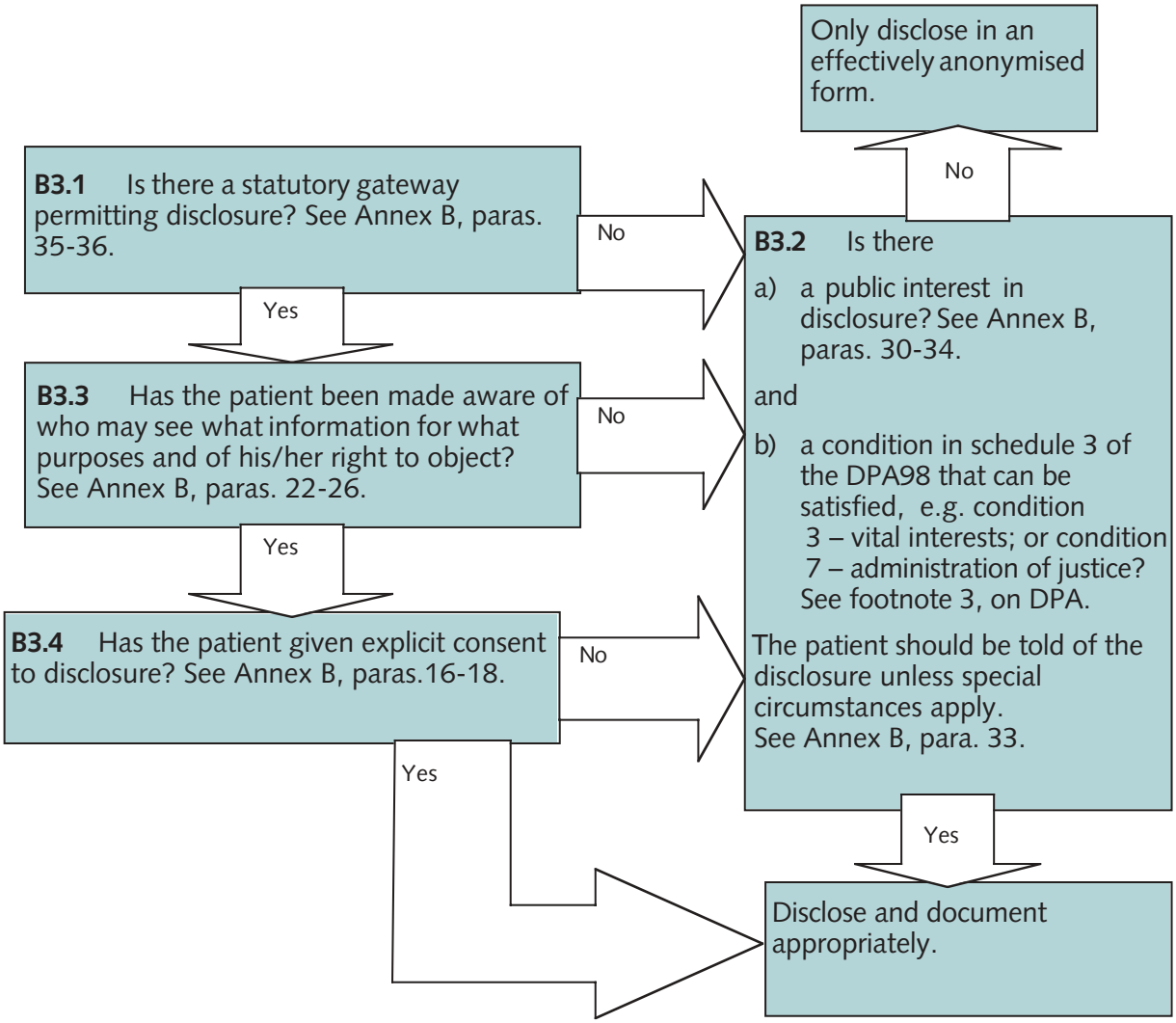


11 The processing of confidential patient information by a NHS body or its staff in order to provide healthcare satisfies schedules 2 and 3 of the DPA98, so no test is included here.

B2: Disclosure Model – where the purpose isn't healthcare but it is a medical purpose as defined in the legislation



B3: Disclosure Model – where the purpose is unrelated to healthcare or another medical purpose



Is it Confidential?

1. A duty of confidence arises when one person discloses information to another (e.g. patient to clinicians) in circumstances where it is reasonable to expect that the information will be held in confidence. It is a legal obligation that is derived from case law, rather than an Act of Parliament, built up over many years and often open to different interpretations. It is also a requirement established within professional codes of conduct and, additionally, there should be specific requirements within NHS employment contracts linked to disciplinary procedures.

2. It is generally accepted that information provided by patients to the health service is provided in confidence and must be treated as such so long as it remains capable of identifying the individual it relates to. This is an important point, as once information is effectively anonymised it is no longer confidential[12].

3. When an individual has died, it is unlikely that information relating to that individual remains legally confidential. However, an ethical obligation to the relatives of the deceased exists and health records of the deceased are public records and governed by the provisions of the Public Records Act 1958. This permits the use and disclosure of the information within them in only limited circumstances. The Access to Health Records Act 1990 permits access to the records of deceased by those with a claim arising out of the individual concerned's death. This right of access is negated however if the individual concerned requested that a note denying access be included within the record prior to death (this might be part of a formal advance directive)[13].

Health Records are for Healthcare

4. Where patients have consented to healthcare, research has consistently shown that they are normally content for information to be disclosed in order to provide that healthcare[14]. However, it is still very important that reasonable efforts are made to ensure that patients understand how their information is to be used to support their healthcare and that they have no objections. Where this has been done effectively, consent can be implied, providing that the information is shared no more widely and that "need to know" principles are enforced. This is particularly important where the use or disclosure of information, whilst an important element of modern healthcare provision, is neither obvious nor easy to understand. It is particularly important to check that patients understand and are content for information to be disclosed to other organisations or agencies contributing to their health care.

5. In many cases the information that needs to be provided to patients, in order for them to understand information disclosures, will be contained within leaflets and booklets made available by all NHS organisations.

6. NHS organisations should have, or should be putting in place, systems and processes that will, over time, restrict the use and disclosure of confidential patient information to those activities that are

---

12 Effective anonymisation generally requires more than just the removal of name and address. Full postcode can identify individuals, NHS Number can be a strong identifier and other information, e.g. date of birth, can also serve as an identifier, particularly if looked at in combination with other data items.

13 For further information on the Public Records Act 1958, The Access to Health Records Act 1990 and others, go to http://www.hmso.gov.uk/acts/

14 E.g. Patient Electronic Record: Information and Consent (PERIC) – Public attitudes to protection and use of personal health information. July 02. School of Health and Related Research, University of Sheffield.

Patient Information and Consent. October 2002. Consumers Association in association with the NHS Information Authority and Health Which?

directly concerned with or support patient healthcare. Further, even within this healthcare environment, organisations must also develop access controls and authentication procedures that give effect to need to know principles.

Consent Issues[15]

Competence to consent[16]

7. Seeking consent may be difficult, either because patients' disabilities or circumstances have prevented them from becoming informed about the likely uses of their information, or because they have a difficulty communicating their decision (be it to consent or object).

a. In the former case, extra care must be taken to ensure that information is provided in a suitable format or language that is accessible (e.g. providing large print or Braille versions of leaflets for those with reading difficulties) and to check that it has been understood.

b. In the latter case, it will be important to check for a clear and unambiguous signal of what is desired by the patient, and to confirm that the interpretation of that signal is correct by repeating back the apparent choice.

8. Failure to support those with disabilities could be an offence under the Disability Discrimination Act 1995, and may prevent consent from being gained. Support for communicating with patients having specific disabilities can be obtained from a range of agencies, e.g.

   a. Royal National Institute for the Blind

   b. Royal National Institute for the Deaf

   c. Disability Rights Commission – www.drc-gb.org

   d. Speakability – www.speakability.org.uk

Children and young people[17]

9. Young people aged 16 or 17 are presumed to be competent for the purposes of consent to treatment and are therefore entitled to the same duty of confidentiality as adults. Children under the age of 16 who have the capacity and understanding to take decisions about their own treatment are also entitled[18] to make decisions about the use and disclosure of information they have provided in confidence (e.g. they may be receiving treatment or counselling about which they do not want their parents to know[19]).

---

15 For further information on consent see http://www.doh.gov.uk/consent/refguide.pdf

16 Competence is understood in terms of the patient's ability to understand the choices and their consequences, including the nature, purpose and possible risk of any treatment (or non-treatment). Detailed guidance on assessing mental capacity can be found at " assessment of mental capacity: guidance for doctors and lawyers (BMA and Law society, 1995)"

17 Detailed guidance can be found in Seeking Consent: Working with Children at http://www.doh.gov.uk/consent/

18 In *Gillick v WestNorfolk and Wisbech Health Authority [1986] AC 112* it was held that, where a child is under 16, but has sufficient understanding in relation to the proposed treatment to give (or withhold) consent, his or her consent (or refusal) should be respected. However, the child should be encouraged to involve parents or other legal guardians.

19 For more detailed guidance on sexual health and contraceptive issues see 'Confidentiality and Young People Toolkit' and 'Guidance for Field Social Workers, Residential Social Workers and Foster Carers on providing information and referring young people to contraceptive and sexual health services'. Both documents are at – http://www.teenagepregnancyunit.gov.uk – under Guidance and Publications.

However, where a competent young person or child is refusing treatment for a life threatening condition, the duty of care would require confidentiality to be breached to the extent of informing those with parental responsibility for the child who might then be able to provide the necessary consent to the treatment.

10. In other cases, consent should be sought from a person with parental responsibility if such a person is available. It is important to check that persons have proper authority (as parents or guardians). Ideally, there should be notes within the child's file as to any unusual arrangements.

Where patients are unable to give consent

11. If a patient is unconscious or unable, due to a mental or physical condition, to give consent or to communicate a decision, the health professionals concerned must take decisions about the use of information. This needs to take into account the patient's best interests and any previously expressed wishes, and be informed by the views of relatives or carers as to the likely wishes of the patient. If a patient has made his or her preferences about information disclosures known in advance, this should be respected.

12. Sometimes it may not be practicable to locate or contact an individual to gain consent. If this is well evidenced and documented and anonymised data is not suitable, the threshold for disclosure in the public interest may be lessened where the likelihood of detriment to the individual concerned is minimal. Where explicit consent cannot be gained and the public interest does not justify breaching confidentiality, then support would be needed under Section 60 of the Health and Social Care Act 2001.See paragraphs 29-34 of this section.

13. Where the patient is incapacitated and unable to consent, information should only be disclosed in the patient's best interests, and then only as much information as is needed to support their care. This might, however, cause unnecessary suffering to the patient's relatives, which could in turn cause distress to the patient when he or she later learned of the situation. Each situation must be judged on its merits, and great care taken to avoid breaching confidentiality or creating difficulties for the patient. Decisions to disclose and the justification for disclosing should be noted in the patient's records. Focusing on the future and care needs rather than past records will normally help avoid inappropriate disclosures.

14. Such circumstances will usually arise when a patient has been unable to give informed consent to treatment, and, provided the patient has not objected, this may justify the disclosure of some information with relatives in order to better understand the patient's likely wishes. There may also be occasions where information needs to be shared with carers in order to assess the impact of disclosures to the patient him or herself. Such occasions are rare and justifiable only in the best interests of the patient.

15. Patients are often asked to indicate the person they would like to be involved in decisions about their care should they become incapacitated. This will normally, but not always, be the 'next of kin'. It should be made clear that limited information will be shared with that person, provided the patient does not object. This gives patients the opportunity to agree to disclosures or to choose to limit disclosure, if they so wish.

Explicit consent

16. When seeking explicit consent from patients, the approach must be to provide:

    a. honest, clear, objective information about information uses and their choices – this information may be multi-layered, allowing patients to seek as much detail as they require;

    b. an opportunity for patients to talk to someone they can trust and of whom they can ask questions;

    c. reasonable time (and privacy) to reach decisions;

    d. support and explanations about any form that they may be required to sign;

    e. a choice as to whether to be contacted in the future about further uses, and how such contacts should be made; and

    f. evidence that consent has been given, either by noting this within a patient's health record or by including a consent form signed by the patient.

17. The information provided must cover:

    a. a basic explanation of what information is recorded and why, and what further uses may be made of it;

    b. a description of the benefits that may result from the proposed use or disclosure of the information;

    c. how the information and its future uses will be protected and assured, including how long the information is likely to be retained, and under what circumstances it will be destroyed;

    d. any outcomes, implications, or risks, if consent is withheld (this must be honest, clear, and objective – it must not be or appear to be coercive in any way); and

    e. an explanation that any consent can be withdrawn in the future (including any difficulties in withdrawing information that has already been shared).

18. The information provided must allow for disabilities, illiteracy, diverse cultural conditions and language differences.

The right to withhold or withdraw consent

19. Patients do have the right to object to information they provide in confidence being disclosed to a third party in a form that identifies them, even if this is someone who might provide essential healthcare. Where patients are competent to make such a choice and where the consequences of the choice have been fully explained, the decision should be respected. This is no different from a patient exercising his or her right to refuse treatment.

20. There are a number of things to consider if this circumstance arises:

    a. The concerns of the patient must be clearly established and attempts made to establish whether there is a technical or procedural way of satisfying the concerns without unduly compromising care.

b. The options for providing an alternative form of care or to provide care through alternative arrangements must be explored.

c. Decisions about the options that might be offered to the patient have to balance the risks, staff time and other costs attached to each alternative that might be offered against the risk to the patient of not providing healthcare.

21. Every effort must be made to find a satisfactory solution. The development of technical measures that support patient choice is a key element of work to determine the standards for electronic integrated care records. Careful documentation of the decision making process and the choices made by the patient must be included within the patient's record.

Informing Patients

22. The Data Protection Act 1998 requires that patients be informed, in general terms, how their information may be used, who will have access to it and the organisations it may be disclosed to. People must also be told who is responsible for their personal information – the 'data controller' – and how to contact them. This should take place prior to the information being used, accessed or disclosed. The requirement falls upon both those who provide information and those who receive it. The obligations of the recipient can be discharged by the provider informing patients of the possible chain of disclosures and uses.

23. The principle that this requirement addresses is that of *Fair Processing* as provided by the 1st Data Protection Principle of the Data Protection Act 1998. Whilst the specific legal requirement is limited to the general information outlined above, it clearly makes sense to ensure that all the information that needs to be communicated to patients is addressed at the same time. In particular, the additional information needed to support patient choice and awareness of rights (para 26 below) should not, in practice, be dealt with separately.

24. There are specific exemptions to the requirement in the Data Protection Act to provide fair processing information, though not to the information needed to support choice and common law rights (see below). Fair processing information does not have to be provided by a NHS body that has been given identifiable information about an individual by a third party, i.e. it is not obtained directly from the individual, in two specific cases. The first is where there is a legal requirement to hold or process the information, and the second is where providing the fair processing information would require disproportionate effort. Advice on whether disproportionate effort might apply can be obtained from the Office of the Information Commissioner at www.informationcommissioner.gov.uk.

25. It is good practice to inform patients where

a. Section 60 of the Health & Social Care Act 2001 has been used to set aside common law confidentiality requirements and

b. an exemption to the fair processing requirements of the DPA98 has applied,

There is however, no requirement to do so if this would require disproportionate effort.[20] Advice on this should be sought from the Data Protection officer or Caldicott Guardian.

20 The Information Commissioner offers guidance as to the meaning of the phrase 'disproportionate effort'. See www.informationcommissioner.gov.uk.

26. Where patients are to be offered choice about how information that relates to them might be used, they must also be made aware of their right to impose restrictions. Although this right will be provided in most circumstances by the common law of confidentiality rather than the Data Protection Act, it will generally be appropriate for patients to be told about their rights at the same time as they are provided with information on proposed uses.

Common Law and disclosure in the Public Interest

27. The key principle of the duty of confidence is that information confided should not be used or disclosed further in an identifiable form, except as originally understood by the confider, or with his or her subsequent permission. NHS organisations should have, or be putting in place, procedures for reviewing the appropriateness and necessity of using confidential patient information to support specific purposes. They should also be developing staff codes of practice and putting in place information sharing protocols to govern working across organisational boundaries.

28. There are exceptions to the duty of confidence that may make the use or disclosure of confidential information appropriate. Statute law requires or permits the disclosure of confidential patient information in certain circumstances, and the Courts may also order disclosures. Case law has also established that confidentiality can be breached where there is an overriding public interest.

29. In some circumstances however, there is no reasonably practicable way of meeting these common law obligations whilst still effectively satisfying an important requirement. Where this is accepted to be the case by the independent statutory Patient Information Advisory Group (PIAG) it may be possible to use powers provided under section 60 of the Health & Social Care Act 2001 to set aside obligations of confidentiality, in effect replacing them with a regulatory code. When section 60 support is provided it is lawful to share information.

In the 'public interest'/ to protect the public

30. Under common law, staff are permitted to disclose personal information in order to prevent and support detection, investigation and punishment of serious crime and/or to prevent abuse or serious harm to others where they judge, on a case by case basis, that the public good that would be achieved by the disclosure outweighs both the obligation of confidentiality to the individual patient concerned and the broader public interest in the provision of a confidential service.

31. Whoever authorises disclosure must make a record of any such circumstances, so that there is clear evidence of the reasoning used and the circumstances prevailing. Disclosures in the public interest should also be proportionate and be limited to relevant details. It may be necessary to justify such disclosures to the courts or to regulatory bodies and a clear record of the decision making process and the advice sought is in the interest of both staff and the organisations they work within.

32. Wherever possible the issue of disclosure should be discussed with the individual concerned and consent sought. Where this is not forthcoming, the individual should be told of any decision to disclose against his/her wishes. This will not be possible in certain circumstances, e.g. where the likelihood of a violent response is significant or where informing a potential suspect in a criminal investigation might allow them to evade custody, destroy evidence or disrupt an investigation.

33. Each case must be considered on its merits. Decisions will sometimes be finely balanced and staff may find it difficult to make a judgement. It may be necessary to seek legal or other specialist advice (e.g.

from professional, regulatory or indemnifying bodies) or to await or seek a court order. Staff need to know who and where to turn to for advice in such circumstances.

Figure 7: Examples of Disclosure to Protect the Public

Serious Crime[21] and National Security

The definition of serious crime is not entirely clear. Murder, manslaughter, rape, treason, kidnapping, child abuse or other cases where individuals have suffered serious harm may all warrant breaching confidentiality. Serious harm to the security of the state or to public order and crimes that involve substantial financial gain or loss will also generally fall within this category. In contrast, theft, fraud or damage to property where loss or damage is less substantial would generally not warrant breach of confidence.

Risk of Harm

Disclosures to prevent serious harm or abuse also warrant breach of confidence. The risk of child abuse or neglect, assault, a traffic accident or the spread of an infectious disease are perhaps the most common that staff may face. However, consideration of harm should also inform decisions about disclosure in relation to crime. Serious fraud or theft involving NHS resources would be likely to harm individuals waiting for treatment. A comparatively minor prescription fraud may actually be linked to serious harm if prescriptions for controlled drugs are being forged. It is also important to consider the impact of harm or neglect from the point of view of the victim(s) and to take account of psychological as well as physical damage. For example, the psychological impact of child abuse or neglect may harm siblings who know of it in addition to the child concerned.

Other disclosures in the public interest

34. Similarly, when the public good that would be served by disclosure is significant, there may be grounds for disclosure. The key principle to apply here is that of proportionality. Whilst it would not be reasonable and proportionate to disclose confidential patient information to a researcher where patient consent could be sought, if it is not practicable to locate a patient without unreasonable effort and the likelihood of detriment to the patient is negligible, disclosure to support the research might be proportionate. Other factors e.g. ethical approval, servicing and safeguards, anonymisation of records and/or clear deletion policies etc might also influence a decision on what is proportionate. It is important not to equate "the public interest" with what may be "of interest" to the public[22].

Administrative Law

35. The NHS deals with confidential patient information in order to carry out specific functions. In doing so it must act within the limits of its powers. Such powers are often set out in statute and it is important that all NHS bodies be aware of the extent of their powers, in particular any restrictions that this may place on the use or disclosure of confidential information. Where such information is processed outside these powers then the processing may be unlawful.

21 Serious crime, as defined by the GMC is "a crime that puts someone at risk of death or serious harm and would usually be crimes against the person, such as abuse of children" (GMC guidance "Confidentiality: Protecting and Providing Information paragraph 37).

22 See Eleventh Report of the Data Protection Commissioner (1995) Appendix 4.

36. The approach often adopted by Government to address situations where a disclosure of information is prevented by lack of function (the ultra vires rule), is to create, through legislation, new statutory gateways that provide public sector bodies with the appropriate information disclosure function. However, unless such legislation explicitly requires that confidential patient information be disclosed, or provides for common law confidentiality obligations to be set aside, then these obligations must be satisfied prior to information disclosures taking place, e.g. by obtaining patient consent.

Data Protection Considerations

37. The Data Protection Act 1998 provides a framework that governs the processing of information that identifies living individuals – personal data[23] in Data Protection terms. Processing includes holding, obtaining, recording, using and disclosing information and the Act applies to all forms of media, including paper and images.

38. The Data Protection Act prohibits processing unless conditions set out in two particular schedules are met. Schedule 2 conditions apply to all processing whereas Schedule 3 provides additional and more exacting conditions that only apply to the processing of *sensitive personal data*, such as health information. Footnote 3 provides a link to the Data Protection Act 1998, where the Schedule 2 and 3 conditions can be found.

39. It is important to understand the role of consent in relation to these schedules. Whilst consent is one of the conditions in each Schedule that might be satisfied, only one condition in each Schedule needs to be satisfied and NHS bodies processing personal health information for legitimate medical purposes[24] may satisfy a condition in each Schedule without needing to obtain patient consent. Note however that, in addition to these schedules, there is a general requirement, within the Data Protection Act 1st principle, for all processing to be lawful. This includes meeting common law confidentiality obligations, which are likely themselves to require consent to be obtained.

40. The Data Protection Act provides a comprehensive framework of required good practice that extends far wider than confidentiality. Requirements include notification (formerly registration) with the Information Commissioner, commitment to data quality, effective information security and the extension of a range of rights to patients. More information on the Act's requirements can be found at www.informationcommissioner.gov.uk

Human Rights Act 1998

41. Article 8 of the European Convention on Human Rights[25], which is given effect in UK law by the Human Rights Act, establishes a right to 'respect for private and family life'. This may be open to some interpretation in points of detail by the courts in years to come, but it creates a general requirement to protect the privacy of individuals and preserve the confidentiality of their health records. It underpins the Confidentiality Model presented in this code of practice. There are also more general requirements in relation to actions having legitimate aims and being proportionate to the need. Current

23 Personal data is defined under the DPA98 as *'data which relate to a living individual who can be identified – (a) from those data, or (b) from those data and other information which is in the possession of, or likely to be in the possession of, the data controller – and includes any expression of opinion about the individual and any indications of the intentions of the data controller or any other person in respect of the individual'.*

24 Under the DPA98, 'medical purposes' includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.

25 Convention for the Protection of Human Rights and Fundamental Freedoms (4. ix. 1950; TS 71; Cmnd 8969).

understanding is that compliance with the Data Protection Act 1998 and the common law of confidentiality[26] should satisfy Human Rights requirements.

Health & Social Care Act 2001: Section 60

42. Section 60 of the Health and Social Care Act 2001 makes it lawful to disclose and use confidential patient information in specified circumstances where it is not currently practicable to satisfy the common law confidentiality obligations. This does not create new statutory gateways, so the processing must still be for a lawful function, but does mean that the confidentiality obligations do not have to be met, e.g. consent does not have to be obtained. Even where these powers apply however, the Data Protection Act 1998 also continues to apply.

43. This is intended primarily as a temporary measure until anonymisation measures or appropriate recording of consent can be put in place. The Government has made it clear that it will only introduce such requirements where necessary and upon the advice of the independent statutory Patient Information Advisory Group (PIAG). See http://www.doh.gov.ipu/confiden for more details, including guidance on applications for support.

44. Where the powers provided by this legislation are used to support the processing of confidential patient information there will be additional safeguards and restrictions on the use and disclosure of the information. These may differ from case to case and change over time where the process of annual review required by the legislation results in more stringent safeguards being applied.

45. The Health Service (Control of Patient Information) Regulations 2002 were the first regulations to be made under section 60 of this Act, and support the operations of cancer registries and the Public Health Laboratory Services in respect of communicable diseases and other risks to public health.

Legal Restrictions on Disclosure

Sexually Transmitted Diseases (STD)[27]

46. Existing regulations require that every NHS trust and Primary Care Trust shall take all necessary steps to secure that any information capable of identifying an individual obtained by any of their members or employees with respect to persons examined or treated for any sexually transmitted disease (including HIV and AIDS) shall not be disclosed except:

    a. where there is explicit consent to do so;

    b. for the purpose of communicating that information to a medical practitioner, or to a person employed under the direction of a medical practitioner in connection with the treatment of persons suffering from such disease or the prevention of the spread thereof; and

    c. for the purpose of such treatment or prevention.

26 Alternatively, compliance with the DPA98 and the regulatory code that applies where section 60 of the Health & Social Care Act 2001 is used to set aside common law obligations of confidentiality.

27 AIDS (Control) Act 1987; NHS (Venereal Diseases) Regulations 1974; NHS Act 1977, NHS Trusts and Primary Care Trusts (Sexually Transmitted Diseases) Directions 2000. [Legislative amendments are necessary to reflect organisational change.]

47. Whilst the existing regulations do not extend to all NHS and partner organisations [and are currently being reviewed], it is clear that many patients would regard information about STDs as particularly sensitive and private. It should never be assumed that patients are content for this information to be shared unless it has a direct and significant bearing on their healthcare and where the regulations apply it must not be disclosed other than as described in the previous paragraph.

Human Fertilisation & Embryology[28]

48. Disclosure restrictions can also apply to fertilisation and embryo treatments where individuals can be identified. Generally, explicit consent is required, except in connection with the:

    a. provision of treatment services, or any other description of medical, surgical or obstetric services, for the individual giving the consent;

    b. carrying out of an audit of clinical practice; or

    c. auditing of accounts.

Legally required to disclose

49. Some statutes place a strict requirement on clinicians or other staff to disclose information. Care should be taken however to only disclose the information required to comply with and fulfil the purpose of the law. If staff have reason to believe that complying with a statutory obligation to disclose information would cause serious harm to the patient or another person, they should seek legal advice. The main requirements to disclose are detailed on the Department of Health web-site at http://www.doh.gov.ipu/confiden.

50. The courts, including coroner's courts, and some tribunals and persons appointed to hold inquiries have legal powers to require that information that may be relevant to matters within their jurisdiction be disclosed. This does not require the consent of the patient whose records are to be disclosed but he/she should be informed, preferably prior to disclosure. Disclosures must be strictly in accordance with the terms of a court order and to the bodies specified in the order. Where staff are concerned that a court order requires disclosure of sensitive information that is not germane to the case in question, they may raise ethical concerns with the judge or presiding officer. If however the order is not amended it must be complied with.

Legally permitted to disclose

51. Legislation may also create a statutory gateway that allows information to be disclosed by a NHS body where previously it might have been unlawful to do so, e.g. section 115 of the Crime & Disorder Act 1998. This sort of permissive gateway generally stops short of creating a requirement to disclose, therefore the common law obligations of confidentiality must still be satisfied, as must the requirements of the Data Protection Act 1998. Details of current statutory gateways can also be found at http://www.doh.gov.ipu/confiden.

28 Human Fertilisation and Embryology Act 1990: ss 31 & 33;
Human Fertilisation and Embryology (Disclosure of Information) Act 1992.

Annex C – Index of Confidentiality Decisions in Practice

This section provides examples of confidentiality decisions in practice, illustrating how the approach described in the previous section can be used to guide decision-makers.

Model B1 – Disclosures to support or audit healthcare

1. Disclosures to NHS staff involved in the provision of healthcare
2. Disclosures to social workers or other staff of non-NHS agencies involved in the provision of healthcare
3. Disclosures to clinical auditors
4. Disclosures to parents and guardians
5. Disclosures to carers without parental responsibility

Model B2 – Disclosures for other medical purposes

6. Disclosure to researchers
7. Disclosure to NHS Managers and/or the Department of Health, e.g. commissioning, prescribing advisers, financial audit, resource allocation etc
8. Disclosures to Occupational Health Practitioners
9. Disclosures to bodies with statutory investigative powers – GMC, Audit Commission, the Health Service Ombudsman, CHAI
10. Disclosures to NHS Complaints Committees
11. Disclosure to cancer registries

Model B3 – Disclosures for non-medical purposes

12. Disclosure to hospital chaplains
13. Disclosure to non-statutory investigations
14. Disclosure to government departments
15. Disclosure to the police

16. Disclosure required by a court, including a coroner's court, tribunals and inquiries

17. Disclosure to Sure Start Teams

18. Disclosure to the media

19. Disclosure to solicitors

Model B1: Healthcare Purposes

1) To NHS staff involved in the provision of healthcare	Where information has to be shared widely to provide healthcare, additional efforts to ensure that patients are effectively informed should be made.
2) To social workers or other non-NHS staff involved in the provision of healthcare	The test of what would satisfy the requirement to effectively inform (B1.3) should be more demanding than where disclosure is limited to NHS staff as the breadth of the information disclosure is not as obvious to patients and their consent cannot be assumed. Disclosure may lead to confidential information being held outside the NHS in the records of partner organisations. Patients need to be made aware of this and partner organisations also need to be aware that holding health records imposes particular duties and obligations.
3) To clinical auditors	Model B1 applies to internal clinical auditors i.e. within a NHS organisation; B2 to auditors working for a different organisation (even if within the NHS). The evaluation of clinical performance against standards or through comparative analysis, with the aim of informing the management of services, is an essential component of modern healthcare provision. Every effort should be made to ensure that patients are aware that audit takes place and that it is essential if the quality of care they receive is to be monitored and improved.
4) To parents, i.e. those with parental responsibility for patients, and guardians	Young people aged 16 or 17 are presumed to be competent for the purposes of consent to treatment and are therefore entitled to the same duty of confidence as adults. Children under 16 who have the capacity and understanding to take decisions about their own treatment are also entitled to decide whether personal information may be passed on and generally to have their confidence respected.[29] The key issue here is the 'competence' of the child. If the child is competent then their consent is required to disclose and use information. Staff should encourage children to involve parents, particularly where significant decisions need to be made, but should respect the choice made. However, where a child has refused to consent to treatment for a life threatening condition, staff should inform parents and seek their consent (consent for treatment purposes may be given by parents even where a child objects).
5) To carers without parental responsibility	Carers often provide valuable healthcare and, subject to complying with the best practice outlined, every effort should be made to support and facilitate their work. Only information essential to a patient's care should be disclosed and patients should be made aware that this is the case. However, the explicit consent of a competent patient is needed before disclosing information to a carer. The best interests of a patient who is not competent to consent may warrant disclosure.

29 Detailed guidance can be found in Seeking Consent: Working with Children at http://www.doh.gov.uk/consent/

Model B2: Medical purposes other than healthcare

6) To researchers	The use of anonymised data is preferable for research purposes. Where systems that are capable of providing anonymised data sets for researchers do not yet exist, the use of identifiable patient information to support research may well be appropriate and necessary but normally requires explicit patient consent. Whilst patients are generally aware and supportive of research it is not reasonable to assume that they are aware of and consent to each and every research subject or proposal. All research in the NHS or other research involving NHS patients, their tissue and/or data must meet appropriate standards of research governance, including ethical approval from an appropriate ethics committee – a mandatory requirement for all NHS supported research. If a patient cannot be contacted to obtain consent, it should not be assumed that their medical details can be used for research purposes. In some exceptional circumstances, where the research subject is of such significance or a patient cannot be located in order to seek consent, the public interest may justify disclosure. Where explicit consent has not been gained and the public interest does not justify breaching patient confidentiality, the research project needs support under section 60 of the Health & Social Care Act 2001. The Patient Information Advisory Group (PIAG) Secretariat can help clarify uncertain cases.
7) To NHS managers and the Department of Health, e.g. commissioning, prescribing advisors, financial audit, resource allocation etc.	The use of anonymised data is preferable for management purposes but this is not always practicable. Systems that are capable of providing anonymised data sets for management purposes should be developed. Where they do not yet exist, the use of confidential information to support these activities may well be appropriate and necessary, but care should be taken to determine the minimum requirements. Explicit consent is required unless there is (rarely) a robust public interest justification and, in the absence of either, support is required under section 60 of the Health & Social Care Act 2001.
8) To Occupational Health professionals	Staff may be referred to an occupational health department, e.g. as a result of sickness absence or a perceived failure to meet work targets. This could in turn require disclosure of patient information. Explicit consent should be obtained before disclosing. When clinicians are themselves "the patient" the powers of professional regulatory bodies to require disclosure of their health records may apply. See section 10) below.

Model B2: Medical purposes other than healthcare (continued)

9) To bodies with statutory investigative powers – GMC, Audit Commission, The Health Service Ombudsman, CHAI	GMC assessors are entitled to access confidential patient health records under the powers given to them by virtue of the Medical Act 1983 (as amended by other legislation such as the Professional Performance Act 1995 and the Medical Act Amendment Order 2000). Similarly, the Audit Commission Act 1998 provides auditors appointed under that Act with the powers to access health records and, where necessary, patient-identifiable information to further their investigations. It is for Audit Commission auditors and GMC assessors to decide what level of information is necessary for them to fulfil their functions, e.g. access to a complete record containing patient-identifiable information, selected parts or just anonymised information. If staff have concerns about the level of information requested, good practice would be to seek and document the reasons why this is needed. Patients should be informed that disclosure has been required. The Health Service Ombudsman has the same powers as the Courts to disclose information but see their work as falling under "medical purposes." Any request for information from them should be complied with without necessity of obtaining a court order.
10) To NHS Complaints Committees	It is unlikely to be practicable for complaints committees to undertake their work without access to relevant parts of a complainant's medical record, and anonymisation is not practicable. The use of identifiable information is therefore necessary and appropriate. However, the explicit consent of the complainant, and any other patients whose records may need to be reviewed, is required prior to disclosure. It may be necessary to explain to a complainant that their complaint cannot be progressed if they refuse to authorise disclosure. In some circumstances, where the trust of patients in NHS care or patients may be at risk, the public interest may justify disclosure to complaints committees.
11) To Cancer Registries	The United Kingdom Association of Cancer Registries (UKACR) is a "generic" organisation working on behalf of a number of different registries which all serve a common purpose: • monitoring trends in cancer incidence; • evaluating the effectiveness of cancer prevention and screening programmes; • evaluating the quality and outcomes of cancer care; • evaluating the impact of environmental and social factors on cancer risk; • supporting investigations into the cause of cancer; • providing information in support of cancer counselling services for individuals and families at higher risk of developing cancer. UKACR has been granted temporary support under Section 60 of the Health and Social Care Act 2001 to obtain patient identifiable information for use on cancer registry database, without the consent of patients.

Model B3: Non-medical purposes

12) To hospital chaplains	Spiritual care cannot be practicably provided without access to some confidential patient information and this form of care is strongly desired by a proportion of patients. It therefore meets the tests of necessity and appropriateness. However, the explicit consent of patients is required before confidential information is disclosed to chaplains. Where a patient is not competent to consent to disclosure, e.g. due to unconsciousness, the decision rests with those responsible for the provision of care acting in the best interests of the patient. The views of family members about what the patient would have wanted should be given considerable weight in these circumstances.
13) To non-statutory investigations, e.g. Members of Parliament	If an investigation is appropriately authorised, disclosure will meet tests of necessity and appropriateness. The minimum necessary information should be disclosed. There is a balance to be drawn between ensuring that a patient has understood and properly consented to a disclosure of information and needlessly obstructing an investigation. Careful consideration of any written authorisation and prompt action are key, e.g. where an MP states, in writing, that s/he has a patient's consent for disclosure this may be accepted without further resort to the patient.
14) To government departments (excluding the Department of Health which requires information for medical purposes – see B2)	Government departments require a range of information to carry out their functions. There needs to be a statutory gateway to permit desired information disclosure and government departments should ensure that tests of appropriateness and necessity are satisfied.
15) To the police	Whilst the police have no general right of access to health records there are a number of statutes which require disclosure to them and some that permit disclosure. These have the effect of making disclosure a legitimate function in the circumstances they cover. In the absence of a requirement to disclose there must be either explicit patient consent or a robust public interest justification. What is or isn't in the public interest is ultimately decided by the Courts. Where disclosure is justified it should be limited to the minimum necessary to meet the need and patients should be informed of the disclosure unless it would defeat the purpose of the investigation, allow a potential criminal to escape or put staff or others at risk. See footnote 21 for a definition of "serious crime."

Model B3: Non-medical purposes (continued)

16) To the courts, including a coroner's court, tribunals and enquiries	Model B1, question B 0 applies. The courts, some tribunals and persons appointed to hold enquiries have legal powers to require disclosure of confidential patient information. Care needs to be taken to limit disclosure strictly in terms of the relevant order, the precise information requested to the specified bodies and no others. It is permitted to make ethical objections known to a judge or presiding officer, but unless the order is changed compliance is necessary.
17) To Sure Start Teams	Sure Start aims to both provide new services and to reshape and add value to existing services in order to improve the life chances of young children. It is delivered through local partnerships involving local service providers from health, education, social services and other public services, the voluntary sector and local parents and community representatives. Some of Sure Start's activities are healthcare provision, but others are not. NHS bodies have a statutory gateway to support disclosure to Sure Start teams under the NHS Act 1977 where this supports healthcare. Disclosure to a health professional within a Sure Start team to directly and only support healthcare is covered by Model B1. However, where disclosure is also for non-medical purposes (e.g. educational support), it is covered by Model B3 and explicit parental consent is necessary. If confidential patient health information is to be held within the records of partner organisations, parents need to be made aware of this prior to any disclosure. Receiving organisations also need to be aware that holding health information imposes particular duties and obligations with regard to confidentiality.
18) To the media	Under normal circumstances there is no basis for disclosure of confidential and identifiable information to the media. There will be occasions however when NHS organisations and staff are asked for information about individual patients. Examples include: • Requests for updates on the condition of particular patients, e.g. celebrities; • In distressing circumstances, e.g. following a fire or road traffic accident; • In circumstances where a patient or a patient's relatives are complaining publicly about the treatment and care provided. Where practicable, the explicit consent of the individual patient(s) concerned should be sought prior to disclosing any information about their care and treatment, including their presence in a hospital or other institution. Where consent cannot be obtained or is withheld, disclosure may still be justified in the "exceptional" public interest. In distressing circumstances, care should be taken to avoid breaching the confidentiality of patients whilst dealing sympathetically with requests for information. Where a patient is not competent to make a decision about disclosure, the views of family members should be sought and decisions made in the patient's best interests.

Model B3: Non-medical purposes (continued)

	Where information is already in the public domain, placed there by individuals or by other agencies such as the police, consent is not required for confirmation or a simple statement that the information is incorrect. Where additional information is to be disclosed, e.g. to correct statements made to the media, patient consent should be sought but where it is withheld or cannot be obtained disclosure without consent may still be justified in the public interest. The patients concerned and/or their representatives should be advised of any forthcoming statement and the reasons for it. There is a strong public interest in sustaining the reputation of the NHS as a secure and confidential service but there is a competing interest in ensuring that the reputations of NHS staff and organisations are not unfairly and publicly maligned. Disclosures need to be justified on a case by case basis and must be limited to the minimum necessary in the circumstances. In some circumstances a "dignified silence" in the face of media enquiry, may be the best approach for the NHS to take, depending on the nature of the case involved.
19) To Solicitors	Most contacts from solicitors are for subject access requests to medical records for compensation claims which may include: • insurance claims against third parties e.g. following road traffic accidents (RTAs); and • work related claims e.g. for disability awards, early retirement etc. There may also be requests for prosecution purposes in cases of, for example, drink driving, RTAs, GBH and murder enquiries etc. Ideally disclosure should be limited to relevant to the incident concerned. However, if disclosure of the full record is required this should be complied with as long as it is clear that the patient understands that full disclosure will take place and has consented. On occasions when clinicians or NHS organisations face legal challenges, solicitors acting on behalf of a client may require access to a third party's record. In such cases, explicit consent should be sought from any person or persons to which it relates. However, if a patient refuses consent, disclosure may still be warranted in the public interest or where a Court Order to support disclosure without consent has been received. It may be possible for a solicitor to make a public interest argument but this would be difficult to judge and best left to the Courts to decide. In all cases a patient should be notified of the disclosure.

33837 1p 3k Nov 03 (CHE)

If you require further copies of this title quote *33837/NHS Code of Practice: Confidentiality*
DH Publications Orderline
PO Box 777
London SE1 6XH
Tel: 08701 555 455
Fax: 01623 724 524
E-mail: doh@prolog.uk.com

08700 102 870 – Textphone (for minicom users) for the hard of hearing 8am to 6pm Monday to Friday.

33837/NHS Code of Practice: Confidentiality can also be made available on request in braille, on audio-cassette tape, on disk and in large print.

www.doh.gov.uk/