

Llywodraeth Cynulliad Cymru
Welsh Assembly Government

Confidentiality: Code of Practice for Health and Social Care in Wales

WELSH ASSEMBLY GOVERNMENT GUIDANCE
ON
SHARING INFORMATION AND CONFIDENTIALITY



Version: 8.8
Date: August 2005

Executive Summary

Increasing importance has been placed on both the health and social care services in Wales to develop clear guidance on protecting the confidentiality of patients and service users whilst allowing the appropriate exchange of information. Service provision, service development, and the maintenance of full, clear and accurate records all require that information be shared to a greater or lesser extent.

For professionals, the free exchange of information between agencies and individuals is essential if concerns about the welfare of children, young people, and adults of all ages are to be met. Those who use health and social care services are aware of the benefits of providing personal information about their needs once only and ensuring that this is available to the professionals and agencies involved in their assessment, treatment programme, and subsequent care planning and service delivery.

Outcomes of service provision require effective and efficient service commissioning, and this in turn relies on information being exchanged between service providers and agencies.

Patients and service users have a right to be informed of the intended use of their information and be given the choice to provide or withhold their consent (as appropriate). They also have an expectation that their information will be held securely and shared only with those directly associated with their care. The four main requirements to maintain and improve a confidential service are:

- **PROTECT** – look after the patient's or service user's information
- **INFORM** – ensure that individuals are aware of how their information is used
- **PROVIDE CHOICE** – allow individuals to decide, where appropriate, whether their information can be disclosed or used in particular ways

To support these three requirements, there is a fourth:

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

Informing Healthcare and Informing Social Care are the strategies that together set out a vision for transforming health and social care in Wales through the effective use of information services, systems and tools. This fundamentally requires that health and social care professionals work with due regard for the protection of confidential information about patients and service users.

The non-statutory guidance and advice within this code of practice will:

- explain the concept of confidentiality;
- describe how a confidential service should operate;
- provide a **high level** description of the main legal requirements;
- recommend a generic decision support tool for sharing/disclosing information and;
- list examples of particular information disclosure scenarios

Annex A of this document provides guidance and advice on the requirements to provide a confidential service. This section includes guidance on best practice in record keeping and security of personal information.

Annex B provides generic guidance for the disclosure of confidential personal identifiable information. This section includes 3 disclosure model flow charts to assist with decision making. You will note that there are legal and ethical distinctions that differ in each case.

Annex C has been developed specifically as guidance for health and social care professionals. This section provides examples of confidentiality decisions in practice and illustrates how the guidance in Annex B can be applied.

As standards and practice covered in this code of practice continue to change, this is an evolving document and, where appropriate, will need to be supplemented by additional specific legislation and guidance.

TABLE OF CONTENTS

Introduction	1
Confidentiality	3
What is Confidential Personal Information?	3
Disclosing and Using Confidential Personal Information	4
Consent to Disclosure	4
Providing a Confidential Service	6
The Confidentiality Model	6
Protecting Personal Information	7
Informing Effectively	7
Providing Choice	8
Improve Wherever Possible	8
Using and Disclosing Confidential Personal Information	9
Legal Considerations	9
Common Law Of Confidentiality	9
Data Protection Act 1998	9
Human Rights Act 1998	10
Administrative Law	10
Key Questions for Confidentiality Decisions	11
Annex A - Providing a Confidential Service: Detailed Requirements	13
A1 Protect Personal Information	13
Record Keeping Best Practice	14
Keeping Personal Information Secure	15
The Caldicott Principles	18
A2 Informing Effectively	18
A3 Provide Choice	20
A4 Improve Wherever Possible	22
Annex B - Confidentiality Decisions	23
Disclosure Models - Sharing Confidential Information to Provide Health and Social Care	24-26
Is it Confidential?	27
Health Records and the Provision of Health and Social Care	27
Consent Issues	28-31
Informing Patients and Service Users	31
Common Law and Disclosure in The Public Interest	33-34
Administrative Law	35
Data Protection Considerations	35
Human Rights Act 1998	36
Crime and Disorder Act 1998: S 115	36
Learning and Skills Act 2000: S.123-129 And Section 138	36
Health and Social Care Act 2001: Section 60	37
Health and Social Care (Community Health and Standards) Act 2003	37
Legal Restrictions on Disclosure	38
Legally Required to Disclose	39
Legally Permitted to Disclose	39

Annex C	40
Model B1: Health and Social Care Purposes	40
Model B2: Purposes Other Than Direct Health or Social Care	40
Model B3: Non Health or Social Care Purposes	40
Glossary of Terms and References	49

INTRODUCTION

1. This document sets out **non-statutory** guidance on best practice for those who work within or under contract to NHS or local authority social services authorities operating in Wales concerning confidentiality and the consent of patient and social care service users to the use of their health and social care records. This document will replace previous guidance for the NHS (DGM (96)43 – *The Protection and Use of Patient Information*) and is a key component of emerging confidentiality arrangements for the NHS and social care services.
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 and local authority social services staff, the Code is also relevant to anyone working in and around health and social care. This includes staff working in the private and voluntary sectors. The Welsh Assembly Government will seek to make it a condition of financial assistance to voluntary organisations and other health and/or social care service providers that they comply with this Code of Practice. Similarly, local authorities should consider imposing conditions when granting financial assistance or entering into contracts for social care service provision.
3. This document
 - a. explains the concept of confidentiality;
 - b. describes how a confidential service should operate;
 - c. provides a **high level** description of the main legal requirements;
 - d. recommends a generic decision support tool for sharing/disclosing information; and
 - 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, 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 will be supplemented by additional guidance.
6. All parts of the NHS and local authority social services need to establish working practices that effectively deliver the patient/service user confidentiality required by law, ethics, professional codes of practice and policy. The objective must be continuous improvement.
7. All staff should meet the standards outlined in this document, as well as those included within 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.

8. 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.

9. The need for change may apply to many existing systems and processes and it is important that staff know whom – perhaps the Caldicott Guardian¹ or Data Protection Officer– should be informed of any specific problems or barriers to change that are noted.

10. NHS and social services managers need to be able to demonstrate active progress in enabling staff to comply with these standards and practices, identifying resource requirements and related areas of organisation or system change. Those organisations and agencies responsible for monitoring NHS and local authority performance play a key role in ensuring effective systems are in place in NHS and local authority organisations.

11. The NHS will be supported to deliver change through the Strategy Implementation Programme for *Informing Healthcare*. Local authority social services will be able to access similar support through work initiated under the auspices of *Informing Social Care*.

Figure 1 - Confidential Services That Meet the Highest Standards

The Welsh Assembly Government is committed to ensuring that NHS and local authority social services provide confidential services that meet the highest standards. This means ensuring that all patient/service user information is processed fairly, lawfully and as transparently as possible so that the public:

- understand the reasons for processing personal information;
- give their consent, when and where required, for the disclosure and use of their personal information ;
- gain trust in the way the services handle information and;
- understand their rights to access information held about them.

CONFIDENTIALITY

What is confidential personal information?

12. A duty of confidence arises when one person discloses information to another (e.g. patient to clinician, service user or carer to social worker) 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 and local authority employment contracts and arrangements as a specific requirement linked to disciplinary procedures.

13. Patients, service users and carers entrust staff with, or allow staff to gather, sensitive information relating to the health and other personal matters of patients/service users as part of seeking treatment, advice and support. They do so in confidence and they have the legitimate expectation that staff will respect their privacy and act appropriately. In certain circumstances e.g. unconscious, mental illness, patients/service users may lack the competence to be aware of their rights in relation to confidential information 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 and service users is to be retained, that the NHS and social services authorities provide, and are 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 person's health and social care records are made by health and social services providers to support that person's health and social care.

14. One consequence of this is that information that can identify individual patients or service users must not be used or disclosed for purposes other than health or social care 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 - Disclosing Information

Patient and service user 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 or service user 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 personal information

15. It is extremely important that patients and service users are made aware of information disclosures that must take place in order to provide them with high quality care. In particular, activities such as clinical governance, clinical audit, performance measurement and evaluation, while wholly proper components of health and social care provision, might not be obvious to patients and should be drawn to their attention. Similarly, whilst patients and service users may understand that information needs to be shared between members of care teams and between different organisations involved in health and social care 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 bodies outside the NHS or local authority social services.

16. Many current uses of confidential patient/service user information do not contribute to or support the health or social care that a patient or service user receives. Very often, these other uses are extremely important and provide benefits to society e.g. research, protecting the health and well-being of the public, health and social services management and financial audit. However, they are not directly associated with the health and social care that individuals receive and we cannot assume that people who seek health and social care are content for their information to be used in these ways.

Consent to disclosure

17. Patients and service users need to be aware of their right to object to certain uses and disclosures of confidential information that identifies them. In certain cases, if patients or service users choose to prohibit information being disclosed to other health and social care professionals involved in providing care, this may mean that the care provided is limited and, in extremely rare circumstances, that it is not possible to offer certain treatment or other service options. Patients and service users must be informed if their decisions about disclosure could have implications for the provision of future 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; similarly, the ability of social care professionals to provide the best service to clients may be constrained if they are not aware of the full picture of a service user's history and circumstances.

18. Where patients or service users have understood:

- a. the use and disclosure of their information associated with their health and social care; and
- b. the choices they have and the implications of choosing to limit how their information may be used or shared

then explicit consent is not usually required for information disclosures needed to provide that health or social care. Even so, opportunities to check that patients and service users understand what may happen to their

information and that they are content with this may be taken. Special attention should be paid to the issues around child consent.

Further information about the Children and Young People's Framework can be found at www.wales.gov.uk/subchildren/content/partnership/index

19. Where the purpose is not directly concerned with the health and social care of an individual, 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.

20. There are situations where consent cannot be obtained for the use or disclosure of patient or service user identifiable information, yet the benefit to the wider public 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, research and Public Health Services can be used without the consent of patients. The Health and Social Care (Community Health and Standards) Act 2003 confers a general power on National Assembly Inspectorates to require information, documents, records (including personal records) which relate to the provision of healthcare by or for a Welsh NHS body or the discharge by a local authority in Wales of its social services functions.

PROVIDING A CONFIDENTIAL SERVICE

The Confidentiality Model

21. The model outlines the requirements that must be met in order to provide patients and service users with a confidential service. Record holders must inform patients and service users of the intended use of their information and 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:

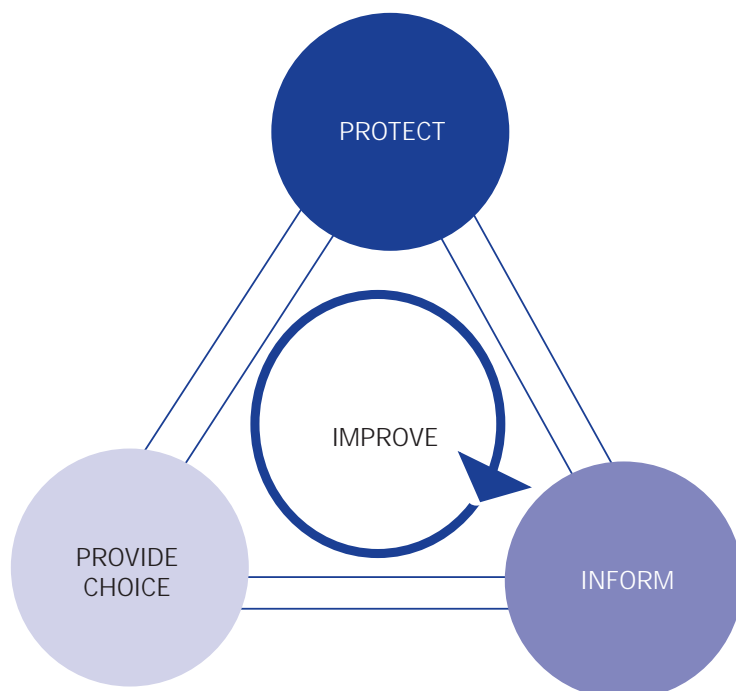
- a. **PROTECT** – look after the patient’s or service user’s information
- b. **INFORM** – ensure that individuals are aware of how their information is used
- c. **PROVIDE CHOICE** – allow individuals to decide, where appropriate, whether their information can be disclosed or used in particular ways

To support these three requirements, there is a fourth:

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

These requirements are depicted in diagrammatic form in Figure 3 and are discussed in the following sections, with additional detail in Annex A.

Figure 3 - Confidentiality Model



Protecting Personal Information

22. Patients' and service users' health, social care and other personal 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 information accurately and consistently
- c. keeping information private
- d. keeping information physically secure
- e. disclosing and using information with appropriate care.

Informing Effectively

23. Patients and service users must be made aware that the information they give may be recorded, may be shared in order to provide them with care, may be used to support clinical or other service audit and other work to monitor the quality of care provided.

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

- a. check where practicable that information leaflets on patient and service user confidentiality and information disclosure have been read and understood. These should be available within each NHS organisation and social services authority;
- b. make clear to patients and service users when information is recorded or health and social care records are accessed;
- c. make clear to patients and service users when they are or will be disclosing information with others;
- d. check that patients and service users are aware of the choices available to them in respect of how their information may be disclosed and used;
- e. check that patients and service users have no concerns or queries about how their information is disclosed and used;
- f. answer any queries personally or direct the patient/ service user to others who can answer their questions or to other sources of information;
- g. respect the rights of patients and service users and assist them with access to their health and social care records.

Providing Choice

25. Patients and service users have different needs and values. This must be reflected in the way they are treated in terms of their medical conditions, their personal and family circumstances and the handling of their personal information. What is very sensitive to one person may be casually discussed in public by another, or something which may not appear to be sensitive may in fact be important to an individual patient and service user in his or her particular circumstances.

26. Staff must:

- a. ask patients and service users before using their personal information in ways that do not directly contribute to or support the delivery of, their care;
- b. respect patients' and service users' decisions to restrict the disclosure or use of information, unless exceptional circumstances apply;
- c. ensure patients and service users understand the implications should they choose to agree to or restrict the disclosure of information.

Improve Wherever Possible

27. NHS and social services organisations and their staff need to work together towards achieving best practice. This means that staff must:

- a. be aware of the issues surrounding confidentiality, and seek training or support where uncertain about dealing with them appropriately;
- b. report breaches or risk of breaches of confidentiality and act appropriately to rectify.

USING AND DISCLOSING CONFIDENTIAL PERSONAL INFORMATION

28. The disclosure and use of confidential personal information needs to be both lawful, ethical and in line with any relevant codes of practice, e.g. Code of Practice for Social Care Workers, Nursing & Midwifery Council Code of Professional Conduct. Whilst law, ethics and professional Codes of Practice 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, while 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, so additional information will be provided as it becomes available. Generally, there are four main areas of law constraining 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 data² in Data Protection terms. Processing includes holding, obtaining, recording, using and disclosing information held in all forms of electronic and paper media, including images. It applies to confidential patient and service user information but is far wider in its scope; for example, it also covers personnel records.

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 handling³. In the context of confidentiality, the most significant principles are:

- the first, which requires processing to be fair and lawful and imposes other restrictions;
- the second, which requires personal data to be processed for one or more specified and lawful purpose(s); and
- the seventh, 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. More information regarding the DPA98 is contained in the Information Commissioner's guidance on the Use and Disclosure of Health Data and can be found at: www.informationcommissioner.gov.uk.pdf

Human Rights Act 1998 (HRA98)

33. Article 8 of the European Convention on Human Rights establishes a right to 'respect for private and family life'. This underscores the duty to protect individual privacy and preserve the confidentiality of health and social care 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 public sector 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 or service user 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 e.g. by obtaining explicit patient or service user consent.

Key Questions for Confidentiality Decisions

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

If the purpose served by disclosing is not healthcare, another medical or social care 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 certain medical and social care 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 health or social care or to assure the quality of that care?

Patients and service users generally understand that some information about them must be shared in order to provide care and treatment, and that clinical or other audit, conducted locally within organisations, is also essential to sustain and improve the quality of care. 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/service user consent each time information is shared⁴.

If not health/social care, is the disclosure to support a broader medical or social care purpose?

Preventative medicine, medical research, health service management and epidemiology, 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. The explicit consent of patients (and of service users in the case of social services authorities) must be sought for identifiable information about them to be disclosed, unless disclosure is authorised, for example, by statute. These provisions include section 60 of the Health and Social Care Act 2001, relevant sections of the Health and Social Care (Community Health and Standards) Act 2003 (sections 74, 100 and s108, the latter giving extra rights to the Assembly under the Care Standards Act 2000); and s119 of the 2003 Act which amends the DPA 1998 in relation to complaints procedures under the 2003 Act and the Children Act 1989.

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

Where the purpose served is not to provide health or social care to an individual 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/service users of proposed disclosures?

There is a specific legal obligation to inform patients and service users in general terms about 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 and service users need to be made aware of their rights and how to exercise them. See Annex B2 for more detail.

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

Explicit consent is required unless disclosure of identifiable information is required by law or the courts, is for a health or social care purpose, can be justified as sufficiently in the public interest to warrant breach of confidence, or is authorised by the statutes mentioned above.

ANNEX A - PROVIDING A CONFIDENTIAL SERVICE: DETAILED REQUIREMENTS

A1 Protect Personal Information

Patients' and service users' 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 of confidentiality, professional obligations, and also staff employment contracts (including those for contractors). Breach of confidence, inappropriate use of health and social care 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 and social care services.

2. Recording personal information accurately and consistently

Maintaining proper records is vital to patient and service user care (see Figure 4). If records are inaccurate, future decisions may be wrong and harmful. 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/service user and the audit of that care, but also to support future research that can lead to better treatment and care 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. ('Recording with Care' published by the Department of Health provides further guidance on case recording policies and practices.)

3. Keeping personal 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 individual concerned. Report breaches or risk of breaches of confidentiality and act appropriately to rectify

Figure 4 - Record Keeping Best Practice

Patient/service user records in the NHS and Social Services Authorities 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 individual.
- 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 service user or carer.
- be clear, unambiguous, (preferably concise) and written in terms that the patient/service user can understand. Abbreviations, if used, should follow common conventions.
- In relation to social care, clarify meaning and understanding of information recorded by reading back what has been recorded to the service user.
- 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

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

and include

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

Patient/service user records should not include

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

4. Keeping personal information physically and electronically secure

This section covers both manual and electronic records. Staff should not leave portable computers, medical notes or case 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 or care records home, and where this cannot be avoided, procedures for safeguarding the information effectively should be locally agreed

Figure 5 - Keeping Personal 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.
- Kept 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.
- Stored and destroyed in line with national guidelines and local retention and destruction policies.

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 need to have 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, and change them at regular intervals to prevent anyone else using them.
- Avoid using short passwords⁵, or using names or words that are known to be associated with them (e.g. children's or pet names or birthdays).
- Always clear the screen of a previous patient or service user's information before seeing another.
- Use a password-protected screen-saver to prevent casual viewing of patient/service user information by others.

5. Disclosing personal information with appropriate care

a. Follow any established information sharing protocols.

NHS and social care 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/service user 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/service user through impersonation by those seeking information improperly. If in doubt firstly check that they have a legitimate right to have access to that information, ask for official identification and/or check telephone number using an independent source and call the person back.

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

Care must be taken, particularly with confidential clinical and personal care information, to ensure that the means of transferring it from one location to another are as secure as they can be.

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 file is generally needless and inefficient (for both parties), and is likely to constitute a breach of confidence.

The Caldicott principles (which were developed for medical purposes, but are adapted below to include social care) should be followed –

Figure 6 - The Caldicott Principles

- i. Justify the purpose.
- ii. Don't use patient/service user identifiable information unless it is absolutely necessary.
- iii. Use the minimum necessary patient/service user identifiable information.
- iv. Access to patient/service user 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.

A2 Informing Effectively

Patients and service users 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 and performance audit and other work to monitor the quality of care provided.

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

6. Check that patients/service users have seen the available information leaflets

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

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

Professional staff too could check that the patient/service user 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 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 people properly.

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

- a. Patients/service users may know little about how the NHS, social services and related agencies work– factors that staff may take for granted. Staff must ensure that patients/service users 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/the housing department/the education department to let them know about your medical history/situation/ concerns...'*; or
 - ii. with electronic records, *'The hospital specialist/the social worker is able to view your records to understand your (medical) history and the tests we have arranged to date before he/she examines/meets with you'*; or
 - iii. in respect of other agencies – *'I will inform Social Services/your family doctor/your consultant about (the matters you have raised)'*.
- b. There are certain Acts of Parliament that require disclosure. Court orders may also require a disclosure. The amount of information disclosed should always be proportionate to the actual need. Even though the patient/service user 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/service users are aware of the choices available in respect of how their information may be used or shared

Patients/service users 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/service users have no concerns or queries about how their information is used

- a. It is important that patients/service users 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/service user 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/service users to others who can answer their questions or other sources of information

- a. It is much better for patients/service users if their concerns can be addressed immediately, but, if staff cannot answer the questions properly, they must refer the patient/service user to a better source of information. Most organisations should have arranged back-up contacts for further information e.g. Community Health Councils.
- b. In some areas of health care provision, 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/service users to have access to their health/care records

Patients have a right to see and/or have copies of their health and social care records under the Data Protection Act 1998.

13. Communicate effectively with patients/service users to help them understand

It is important to recognise the different communications needs of particular individuals. While some may read NHS and social services' authorities leaflets when waiting for assessment and/or 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

Patients/service users have different needs and values, and this must be reflected in the way they are treated, both in terms of their medical condition, social care needs 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/service user in his or her particular circumstances. Patients/service users 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 other purposes.

Although these may generate greater concern, the disclosure of information for health and social care purposes is not normally an issue for the great

majority of patients/service users. Even this cannot be taken for granted and patients/service users must be given opportunities to raise objections and concerns. The development of a truly confidential service will maximise patient/service user trust and minimise the number of objections raised. Whilst it is necessary to disclose information about a patient/service user to those staff who are providing or auditing the standard of care, it is important to ensure that those who see information have a genuine need to know. Staff must:

14. Ask patients/service users 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/service users is required, but does not satisfy the tests of necessity and appropriateness that must govern the use of identifiable information, then it should be anonymised to protect the patient/service user.
- 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'/service users' decisions to restrict the disclosure and/or use of information⁶

- a. In some cases, it may not be possible to restrict information disclosure without compromising care. This would require careful discussion with the patient/service user, but ultimately the patient/service user's choice must be respected.
- b. In the short-term it may not be possible to meet some patients/service users' requests directly though, with some imagination, a compromise arrangement may be possible. This may require discussion about where the patient/service user'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/service users. When constraints are imposed by patients/service users it is important to demonstrate that neither patient/service user safety, nor clinical responsibility for health or social care provision, has been neglected.
- d. Further information regarding patient /service users rights to prevent personal data from being processed if they feel the processing is likely to cause them or someone else to suffer unwarranted substantial damage, harm or distress can be found on the Information Commissioners Website at www.informationcommissioner.gov.uk

16. Explain the implications of disclosing and not disclosing

- a. In order to make valid choices patients/service users must not only know what their options are, but also what are the consequences of making those choices. Explanations must be proportionate to the risks involved and reflect, where possible, the patient/service user's particular circumstances.
- b. Where patients/service users insist on restricting how information may be used or shared in ways that compromise the health or care service's ability to provide them with high quality care, this should be documented within the patient/service user's record. It should be made clear to the patient/service user that they are able to change their mind at a later point.

A4 Improve wherever possible

NHS and social services organisations and their staff need to work together towards achieving best practice. NHS and social services organisations must ensure that their confidentiality procedures are regularly reviewed and remain consistent with prevailing policy. 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 Data Protection Officer or IT Security manager. 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 to protect individuals reporting abuses, as well as NHS and social services authority procedures to support this where necessary (individual 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.

ANNEX B - CONFIDENTIALITY DECISIONS⁷

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.

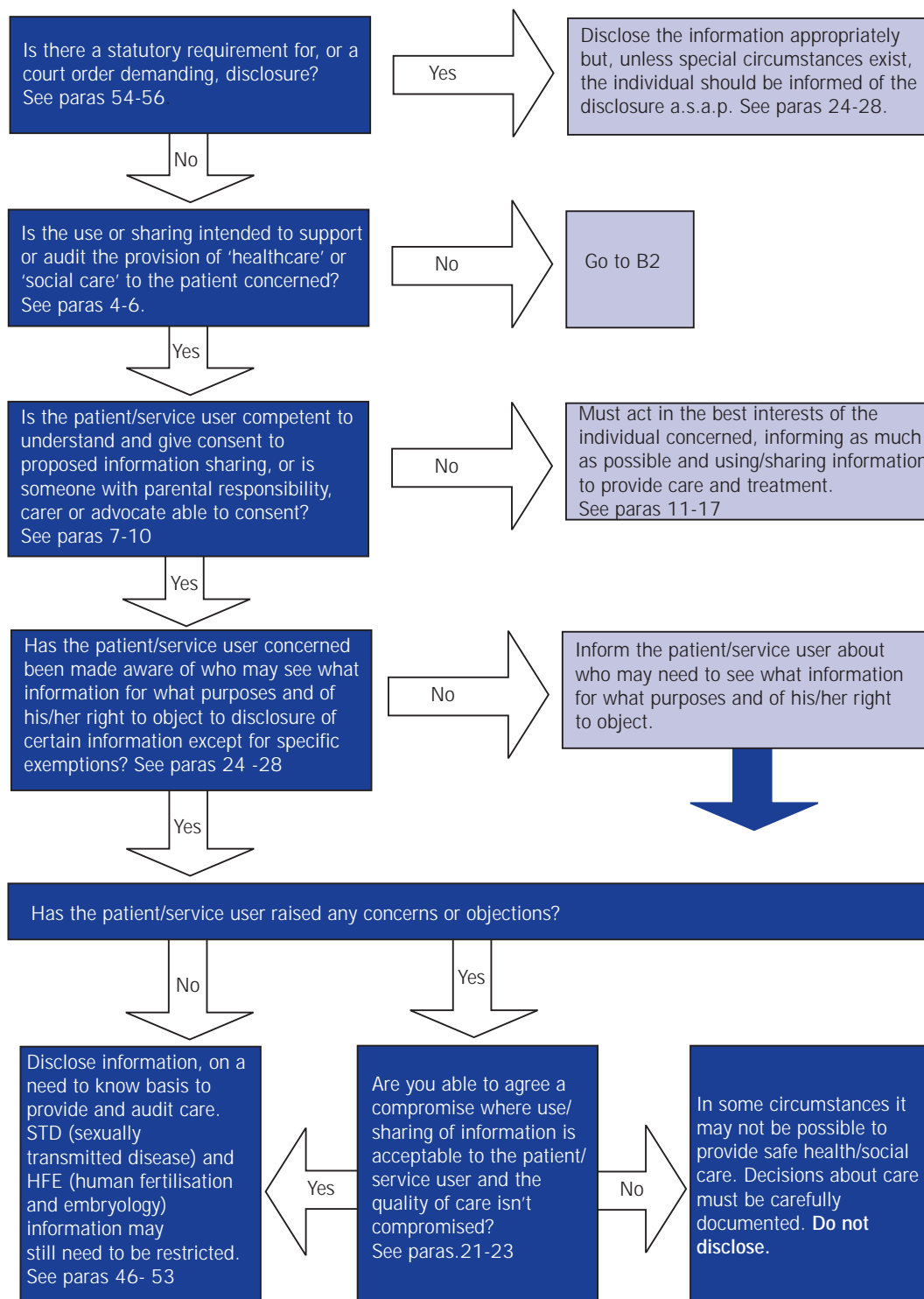
A range of information disclosure scenarios can be found in Annex C. These reference and illustrate the model provided here and can be used to aid decision-making. They highlight issues relating to particular decisions, e.g. disclosure to managers or to the police. It is hoped that they cover many of the circumstances that staff currently have to deal with.

The model is in three parts:

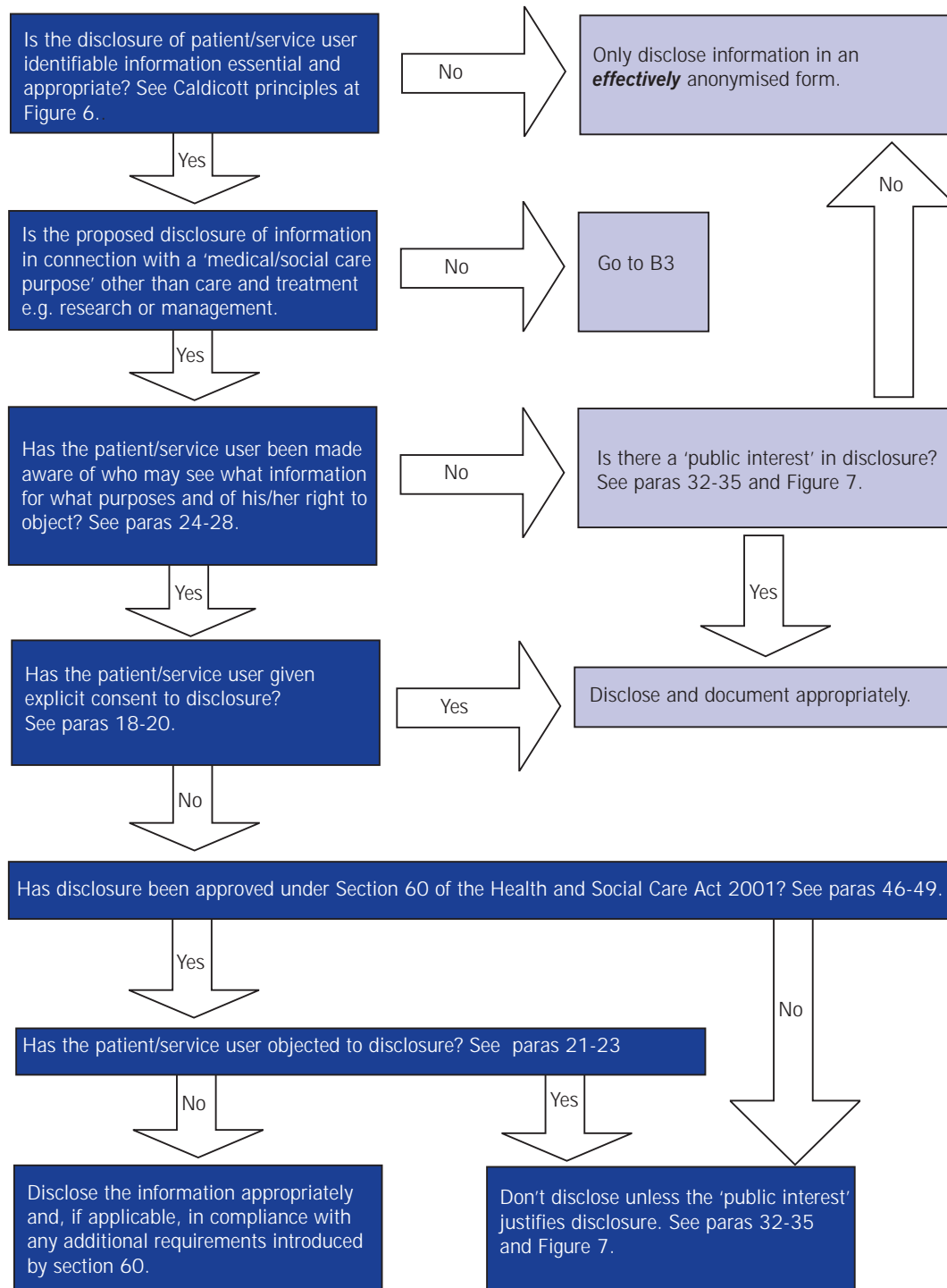
- B1** where it is proposed to disclose confidential information in order to provide health and/or social care
- B2** where the purpose is not health or social care but is a purpose as defined in legislation
- B3** where the purpose is unrelated to healthcare, social care or another medical purpose.

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

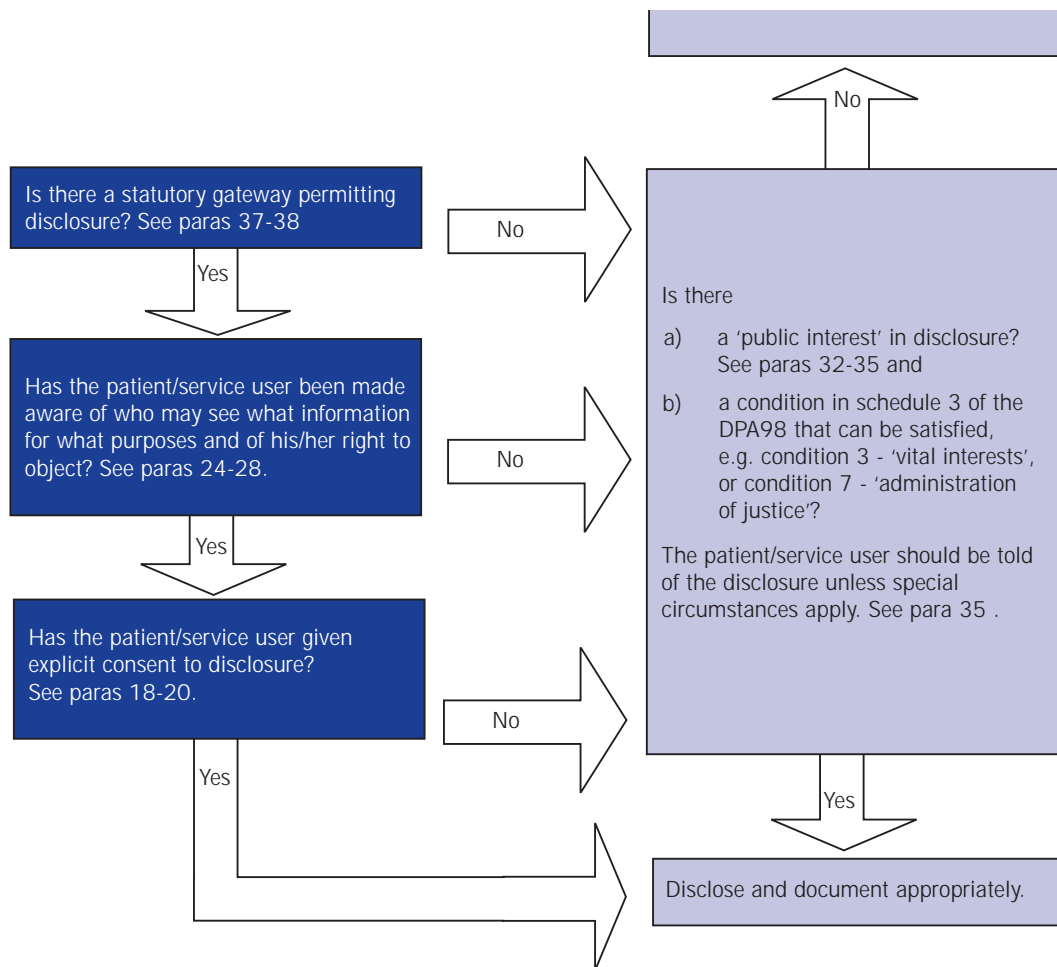
B1: Disclosure Model - where it is proposed to share confidential information in order to provide health or social care



B2: Disclosure Model - where the purpose is not health or social care but it is a purpose as defined in the legislation



B3: Disclosure Model - where the purpose is unrelated to healthcare, another medical purpose or social care



Is it Confidential?

1. A duty of confidence arises when one person discloses information with another (e.g. patient to clinicians, service user to social worker) 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 and social services authorities employment contracts linked to disciplinary procedures.
2. It is generally accepted that information provided by patients/service users to the health or social care services 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 confidential⁸.
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)⁹.

Health and Social Care Records and the Provision of Health and Social Care Services

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. 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. This approach readily applies to the provision of social care services. Where clear explanations have been given to patients/service users about the use of the information, 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 health and social care provision, is neither obvious nor easy to understand. It is particularly important to check that patients/service users understand and are content for information to be disclosed to other organisations or agencies contributing to their care.
5. In many cases the information that needs to be provided to patients/service users, in order for them to understand information disclosures, will

be contained within leaflets and booklets made available by all NHS and social services authorities.

6. NHS organisations and social services authorities should have, or be putting in place, systems and processes that will, over time, restrict the use and disclosure of confidential patient/service user information to those activities that are directly concerned with or support health and social care service provision. Further, even within this environment, organisations must also develop access controls and authentication procedures that give effect to 'need to know' principles.

Consent Issues¹⁰

Capacity to consent¹¹

7. Seeking consent may be difficult, either because patients/service users' 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/service user, 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/service users having specific disabilities can be obtained from a range of agencies, e.g.

- a. Wales Council for the Blind.
- b. Royal National Institute for the Deaf - Wales.
- c. Disability Rights Commission - www.drc-gb.org.

Children, young people and consent to treatment

9. Young people aged 16 or 17 are presumed to be competent for the purposes of consent to health 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 entitled¹⁸ 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^{12 & 13}). 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/service users are unable to give consent

11. If a patient/service user is unconscious or unable, due to a mental or physical condition, to give consent or to communicate a decision, the care professionals concerned must take decisions about the use of information. This needs to take into account the patient/service user's best interests and any previously expressed wishes, informed by the views of relatives, advocates or carers as to the likely wishes of the person. If an individual has made his or her preferences about information disclosures known in advance e.g. advance directive (see paragraph 16), this should be respected.

12. Sometimes it may not be practicable to locate or contact an individual to gain consent. Although this will be subject to individual judgement, where 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 considered to be minimal.

13. 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 30-34 of this section.

14. Where the patient/service user is incapacitated and unable to consent, information should only be disclosed in that person's best interests, and then only as much information as is needed to support their care. This might, however, cause unnecessary suffering to their relatives, which could in turn cause distress to the patient/service user 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 person concerned. Decisions to disclose and the justification for disclosing should be noted in the patient/service user's records. Focusing on the future and care needs rather than past records will normally help avoid inappropriate disclosures. Further guidance on the complex issues that the 'capacity to consent' can raise is to be found in the 'Reference Guide for Consent to Examination or Treatment' (NB :Welsh Assembly Government will shortly be updating its advice in line with Mental Capacity Act 2005 and recent case law)

15. Such circumstances will usually arise when a patient/service user has been unable to give informed consent to treatment. Provided the person has not objected, this may justify the disclosure of some information to relatives

/advocate in order to better understand their 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 person him or herself. Such occasions are rare and justifiable only in the best interests of the patient/service user eg. bad news situations.

16. Where service users have indicated through an Advance Directive (or similar instrument) their preferences with respect to confidentiality issues, it would be good practice to act in accordance with those preferences.

17. Patients/service users 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/service user does not object. This gives individuals the opportunity to agree to disclosures or to choose to limit disclosure, if they so wish.

Explicit consent

18. When seeking explicit consent from patients/service users 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/service users to seek as much detail as they require,
- b. an opportunity for patients/service users 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. 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/service user's health record or by including a consent form signed by the patient/service user.

19. 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).

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

The right to withhold or withdraw consent

21. Patients/service users 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 health or social care. Where individuals 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/service user exercising his or her right to refuse treatment or care.

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

- a. The concerns of the patient/service user 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/service user have to balance the risks, staff time and other costs attached to each alternative that might be offered against the risk to the patient/service user of not providing health and/or social care.

23. Every effort must be made to find a satisfactory solution.

The development of technical measures that support patient/service user choice is a key element of work to determine the standards for the single record under Informing Healthcare and Informing Social Care. Careful documentation of the decision making process and the choices made by the patient/service user must be included within the patient/service user's record.

Informing Patients and Service Users

24. The Data Protection Act 1998 requires that individuals 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/service users of the possible chain of disclosures and uses.

25. 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/service users is addressed at the same time. In particular, the additional information needed to support patient/service user choice and awareness of rights (para 26 below) should not, in practice, be dealt with separately.

26. 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 or social services authority 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.

27. It is good practice to inform patients/service users where

a) an exemption to the fair processing requirements of the DPA98 has been applied,

or

b) where legislation authorises disclosure. Such legislation includes section 60 of the Health and Social Care Act 2003, relevant sections of the Health and Social Care (Community Health and Standards) Act 2003 (sections 74, 100 and s108, the latter giving extra rights to the Assembly under the Care Standards Act 2000); and s119 of the 2003 Act which amends the DPA 1998 in relation to complaints procedures under the 2003 Act and the Children Act 1989.

There is however, no requirement to do so if this would require disproportionate effort.¹⁴ Advice on this should be sought from the Data Protection Officer.

28. Where patients/service users 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/service users 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

29. 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 and social services organisations should have, or be putting in place, procedures for reviewing the appropriateness and necessity of using confidential 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.

30. 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 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.

31. In some circumstances however, there is no reasonably practicable way of meeting these common law obligations. 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 and 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

32. 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.

33. 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.

34. 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.

35. 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. In the case of a local authority, staff should seek advice from the authority's lawyers.

Figure 7 - Disclosures to Protect the Public

Example

Serious Crime¹⁵ 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, for example, could be harmful to 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

36. 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/service user information to a researcher where consent could be sought, if it is not practicable to locate an individual without unreasonable effort and the likelihood of detriment to the patient/service user 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.

Administrative Law

37. The NHS and social services authorities deal with confidential patient/service user 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 and social services authorities are 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.

38. 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/service user 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/service user consent.

Data Protection Considerations

39. The Data Protection Act 1998 provides a framework that governs the processing of information that identifies living individuals – personal data 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.

40. 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.

41. 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 and social care bodies processing personal health and social care information for legitimate medical and care purposes may satisfy a condition in each Schedule without needing to obtain patient/service user 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.

42. 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

43. Article 8 of the European Convention on Human Rights, 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 understanding is that compliance with the Data Protection Act 1998 and the common law of confidentiality should satisfy Human Rights requirements.

Crime and Disorder Act 1998: Section 115

44. Section 115 authorises (but does not require) relevant authorities to disclose information where it is 'necessary or expedient' for the purposes of any provision of the Crime and Disorder Act 1998 to disclose information without the consent of the person to whom it relates. Relevant authorities include local authorities, health authorities and police authorities. The purposes of the Act cover amongst other things, the prevention and reduction of crime and the identification and apprehension of offenders or suspected offenders. The responsibility to disclose relevant information under Section 115 overrides the common law duty of confidence. Any information obtained can only be used for the purposes of the Act with the minimum amount to fulfil the statutory duty being disclosed on a need to know basis. Prevention and detection of crime and the apprehension and prosecution of offenders are also an exception under Section 29 of the Data Protection Act 1998 to the general principle that personal information should not be disclosed.

Learning and Skills Act 2000: Sections 123 - 129 and Section 138

45. The National Assembly has powers to direct local authorities in Wales to provide youth support services for all 11 to 25 year olds, a) to secure the provision of youth support services from others and, b) to participate in the provision of youth support services with others. Section 126 of the Learning and Skills Act 2000 sets out the duties on maintained schools, and educational establishments to provide information to youth support service providers. Information other than the name and address of any pupil or student and the parent of any pupil or student cannot be provided if the young person (or in the case of an under 16-year old, his or her parent) has instructed the institution not to disclose that information. Section 128 provides that the Chief Inspector of Schools will have reasonable right of access to the premises being inspected, including access to information

held on computers. Section 138 enables a Chief Officer of Police, National Council for Education and Training in Wales, Probation Board and Youth Offending Team to supply information about a young person to a local authority or any other person or body involved in the provision of youth support services in Wales.

Health and Social Care Act 2001: Section 60

46. Section 60 of the Health and Social Care Act 2001 makes it lawful to disclose and use confidential patient/service user 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.

47. 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 PIAG. PIAG is supported through the Department of Health - see <http://www.doh.gov.uk/ipu/confiden> for more details, including guidance on applications for support.

48. Where the powers provided by this legislation are used to support the processing of confidential patient/service user 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.

49. 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.

Health and Social Care (Community Health and Standards) Act 2003

50. Part 2 of this Act deals with matters relating to quality and standards in health and social care. Section 51 gives the Commission for Healthcare Audit and Inspection (CHAI) a function of conducting reviews across England and Wales of health care generally or of particular kinds of healthcare. Section 55 of this Act enables the CHAI to review the quality of any data collected by others on healthcare provided by and for the NHS bodies. Sections 70 to 74 gives the Assembly the function of conducting reviews of and investigations into, the provision of health care by and for Welsh NHS bodies and access to the necessary information and documents. Section 94 authorises the Assembly to carry out reviews and investigations concerning the discharge of local authorities' social services functions. In order to

discharge these functions effectively the Assembly may at any time require the provision of any information, documents, records (including personal records) or other items relating to the provision of health and/or social care. The power to require the provision of records includes, in relation to records kept by means of a computer, power to require the provision of the records in legible form. An appropriately authorised person may if it considered necessary or expedient may inspect, take copies of and remove from the premises any documents or records (including personal records) relating to the discharge of health or social services functions. Failure to comply with these requirements without a reasonable excuse is an offence

Legal Restrictions on Disclosure

Sexually Transmitted Diseases (STD)¹⁶

51. Existing regulations require that every NHS Trust and Local Health Board 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.

52. 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 & Embryology¹⁷

53. 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

54. 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/service user or another person, they should seek legal advice.

55. 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

56. Legislation may also create a statutory gateway that allows information to be disclosed by a NHS or social services authority where previously it might have been unlawful to do so, e.g. section 115 of the Crime and 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.

ANNEX C

The material in this section has been developed specifically for the guidance of health and social care professionals to provide examples of confidentiality decisions in practice. They illustrate how the approach described in the previous section can be used to guide decision-makers in the two areas of service.

Model B1 – Disclosures to support or audit health and social care services.

1. Disclosures to NHS and social care staff involved in the provision of health and social care
2. Disclosures to clinical auditors and service regulators
3. Disclosures to parents and guardians
4. Disclosures to carers without parental responsibility

Model B2 – Disclosures for purposes other than direct health or social care purposes.

5. Disclosure to researchers
6. Disclosure to NHS and/or social services authority Managers and/ or the Department of Health or Welsh Assembly Government, e.g. commissioning, prescribing advice, financial audit, resource allocation
7. Disclosures to Occupational Health Practitioners
8. Disclosures to bodies with statutory investigative powers – GMC, Audit Commission Wales, Health Service Ombudsman, CSIW
9. Disclosure for complaints investigation
10. Disclosure to cancer registries

Model B3 – Disclosures for non health or social care purposes.

11. Disclosure to hospital chaplains
12. Disclosure to non-statutory investigations
13. Disclosure to government departments
14. Disclosure to the police
15. Disclosure required by a court, including a coroner's court, tribunals and inquiries
16. Disclosure to Children's and Young People's Partnerships
17. Disclosure to the media
18. Disclosure to solicitors

Model B1: Health and Social Care Purposes	
1) To NHS and Social Care staff involved in the provision of health and social care services	Where information has to be shared widely to provide health and social care, additional efforts to ensure that individuals are effectively informed should be made.
2) To clinical auditors and service regulators	<p>Model B1 applies to internal clinical auditors i.e. within a NHS or social care organisation; B2 to auditors working for a different organisation.</p> <p>The evaluation of service performance against standards or through comparative analysis, with the aim of informing the management of services, is an essential component of modern health and social care provision. Every effort should be made to ensure that patients and service users are aware that audit takes place and that it is essential if the quality of care they receive is to be monitored and improved.</p>
3) To parents and guardians	<p>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.</p> <p>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).</p>
4) To carers without parental responsibility More required	Carers often provide valuable health and social care 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 person's care should be disclosed and individuals should be made aware that this is the case. However, the explicit consent of a competent person is needed before disclosing information to a carer. The best interests of a patient/service user who is not competent to consent may warrant disclosure.

Model B2: Purposes other than direct health or social care

<p>5) To researchers</p>	<p>All research in the NHS and social care services or other research involving NHS patients/social care service users, 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</p> <p>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 personal information to support research may well be appropriate and necessary but normally requires explicit consent. Whilst people 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.</p> <p>If a person cannot be contacted to obtain consent, it should not be assumed that their personal details can be used for research purposes</p> <p>In some exceptional circumstances, where the research subject is of such significance or a person cannot be located in order to seek consent, the public interest may justify disclosure</p> <p>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 and Social Care Act 2001. The PIAG Secretariat can help clarify uncertain cases</p>
<p>6) To NHS and social service authority managers and the NHS Wales Department, e.g. commissioning, prescribing advice, financial audit, resource allocation etc.</p>	<p>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.</p> <p>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 and Social Care Act 2001.</p>

7) Occupational Health Practitioners	<p>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.</p> <p>This could in turn require disclosure of patient information. Explicit consent should be obtained before doing so.</p> <p>When clinicians are themselves “the patient” the powers of professional regulatory bodies to require disclosure of their health records may apply. See section 8 below.</p>
8) To bodies with statutory investigative powers.	<p>From 1st April 2006, the Public Audit (Wales) Act 2004 will provide powers to the Auditor General for Wales to audit health bodies in Wales.</p> <p>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.</p> <p>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.</p> <p>Patients should be informed that disclosure has been required.</p> <p>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.</p>

9) Complaints investigation.	<p>It is unlikely to be practical for persons authorised to investigate complaints to undertake their work without access to relevant parts of a complainant's medical or social care record, and anonymisation is not practicable. The use of identifiable personal information is therefore necessary and appropriate.</p> <p>However, the explicit consent of the complainant, and any other persons 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 to the person charged under the regulations with consideration of complaints.</p> <p>There are some limited circumstances where the public interest may justify disclosure of information. In addition, s119 of the Health and Social Care (Community Health and Standards) Act 2003 exempts from the subject information provisions of the Data Protection Act 1998 the application of those provisions to the personal data where this would be likely to prejudice the proper investigation of the complaint.</p>
10) To Cancer Registries	<p>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:</p> <ul style="list-style-type: none"> - 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. <p>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. This includes the Welsh Cancer Intelligence and Surveillance Unit.</p>

Model B3: Non Health or Social Care Purposes

11) To hospital chaplains	<p>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.</p> <p>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.</p>
12) To non-statutory investigations, e.g. Members of Parliament, Assembly Members	<p>If an investigation is appropriately authorised, disclosure will meet tests of necessity and appropriateness. The minimum necessary information should be disclosed.</p> <p>There is a balance to be drawn between ensuring that a person 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 or AM states, in writing, that s/he has an individual's consent for disclosure this may be accepted without further resort to the person concerned.</p>
13) To government departments (excluding the NHS Wales Department which requires information for medical purposes – see B2)	<p>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.</p>
14) To the police	<p>Whilst the police have no general right of access to health or social care 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.</p> <p>In the absence of a requirement to disclose there must be either explicit consent or a robust public interest justification. What is or isn't in the public interest is ultimately decided by the Courts.</p>

	Where disclosure is justified it should be limited to the minimum necessary to meet the need and individuals 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".
15) To the courts, including a coroner's court, tribunals and enquiries	The courts, some tribunals and persons appointed to hold enquiries have legal powers to require disclosure of confidential personal 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.
16) To Children's and Young People's Partnerships	Children's and Young People's Partnerships provide a forum for co-ordinated planning and delivery of services and to ensure that a network of provision exists in every area that best meets the needs of local young people. They bring together a range of providers to create an integrated and coherent service providing information, advice, guidance, and opportunities to young people between the ages of 11 and 25, where and when they need them. The underlying principle for the exchange of information is the benefit of the young person concerned though that alone is not sufficient justification for disclosing information. Information sharing is considered to be essential but other than where information is processed as a condition of derived statutory powers the information exchange it must be with the informed consent of the individual, on a 'need to know' basis, dependent on a set of administrative triggers and regulated through an authorising officer. The National Assembly Guidance for Young People's Partnerships on 'Information Sharing' should be consulted for further advice. For further information see www.wales.gov.uk/subchildren/
17) 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 and Social Services Authorities and their staff are asked for information about individuals. Examples include:

- Requests for updates on the condition or circumstances of particular individuals, e.g. celebrities;
- In distressing circumstances, e.g. following a fire or road traffic accident;
- In circumstances where a person's relatives are complaining publicly about the treatment, care or service provided.

Where practicable, the explicit consent of the person concerned should be sought prior to disclosing any information about their care, treatment, service or circumstances, including their presence in a hospital or other location. 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 person's confidentiality whilst dealing sympathetically with requests for information. Where a person is not competent to make a decision about disclosure, the views of family members should be sought and decisions made in the person's best interests.

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, a person's consent should be sought. Where it is withheld or cannot be obtained disclosure without consent may still be justified in the public interest. The people 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 and Social Services Authorities as secure and confidential services but there is a competing interest in ensuring that the reputations of both the staff and the organisations are not unfairly and publicly maligned. Disclosures need to be justified on a case by case basis and

	<p>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, depending on the nature of the case involved.</p> <p>In the case of absconders from health or local authority care settings it is imperative that all employees are made fully aware of and follow local policy and protocols where an individual could be considered at risk and disclosure of appropriate information is considered in best interests of individual and/or public</p>
18) To Solicitors	<p>Most contacts from solicitors are for subject access requests to medical or social care records for compensation claims which may include:</p> <ul style="list-style-type: none">- insurance claims against third parties e.g. following road traffic accidents (RTAs), and- work-related claims e.g. disability awards, early retirement, etc. <p>There may also be requests for prosecution purposes in cases of, for example, drink driving, RTAs, GBH and murder enquiries, etc.</p> <p>Ideally disclosure should be limited to information 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.</p> <p>On occasions when clinicians or NHS and social services authorities face legal challenges, solicitors acting on behalf of a client may require access to third parties’ records. In such cases, explicit consent should be sought from any person or persons to whom the legal challenge relates.</p> <p>Records managers and others in receipt of requests for disclosure for legal purposes should not assume responsibility for decisions about whether to disclose or not. The matter should normally be referred to the Chief Executive of the organisation and/or to the organisation’s legal advisers.</p> <p>In all cases a patient should be notified of the disclosure.</p>

GLOSSARY OF TERMS AND REFERENCES

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 postcode and any other detail or combination of details that might support identification.

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 generalised 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.

Disclosure

This is the divulging or provision of access to data.

Explicit Consent

An unambiguous expression of agreement. It is a clear and voluntary indication of preference or choice. Usually given orally or in writing in circumstances where the available options and the consequences have been made clear.

Health and Social Care Purposes

These include all activities that directly contribute to the diagnosis, assessment, care and treatment of an individual and the audit/assurance of the quality of the care and services provided. They do not include research, teaching, financial audit and other management activities.

Implied Consent

This means an agreement that has been signalled by behaviour of an informed individual.

Information Sharing Protocols

Documented rules and procedures for the disclosure and use of patient/ service user information, which specifically relates to security, confidentiality and data destruction, between two or more organisations or agencies.

Patient and service user identifiable information

Key identifiable information includes:

- Name, address, full post code, date of birth;
- Pictures, photographs, videos, audio-tapes or other images;
- NHS number, social services record identifiers, and local person identifiable codes;
- Anything else that may be used to identify an individual directly or indirectly. For example, rare diseases, service provision, treatments or statistical analyses that have very low numbers within a small population may allow individuals to be identified.

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.

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 and social services.

Service User

A person who has applied for, is receiving or who may receive a social care service

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), 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 including the private sector, whether or not these are commissioned by Social Services Authorities and includes the provision of support or services intended to promote an independent way of life within the community.

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 For further details see: <http://howis.wales.nhs.uk/caldicott>
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'.
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). There are also two 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 of Sensitive Personal Data (Elected Representatives) Order 2002. Details of both can be found at www.opsi.gov.uk
4. NB: any "other" organisational forms of audit, i.e. across organisations and nationally, require explicit consent.
5. 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>
6. Through the advent of the single electronic records and the objectives of Informing Healthcare and Informing Social Care, NHS and social services authorities' systems should provide sufficient flexibility to meet all reasonable requests.
7. It is assumed within this methodology that the member of staff making a confidentiality decision is working within an organisation that may legitimately process personal information for health or social care purposes, i.e. that this is a legitimate function of the organisation concerned.
8. 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.
9. For further information on the Public Records Act 1958, the Access to Health Records Act 1990 and others, go to <http://www.opsi.gov.uk/acts/>
10. Patient Information and Consent. October 2002. Consumers Association in association with the NHS Information Authority and Health Which? For further information on consent for treatment see <http://howis.wales.nhs.uk/doclib/treatmentgd- e.pdf>

11. Assessment of mental capacity-2nd edition 2004. The law assumes that adults have the mental capacity to make their own decisions. When individuals lose their decision-making ability, steps must be taken to ensure that their rights are safeguarded, and their wishes are given proper weight. For further information: <http://www.bma.org.uk>
12. Detailed guidance can be found in 'Seeking Consent: Working with Children' at <http://howis.wales.nhs.uk/doclib/treatmentgd-e.pdf>
13. The rights of parents in relation to medical matters concerning their children are subject to the ruling of the House of Lords in the case *Gillick v West Norfolk and Wisbech Area Health Authority* [1985]. The case established the importance of children under 16 who are of sufficient age and understanding to be able to consent to certain decisions regarding their health and welfare. It was held that where a child is under 16, if he/she has sufficient understanding of the advice/treatment and her best interests require such advice and/or treatment, parental consent is not required although they should be encouraged to involve their parents or guardian.

The court can, however, override the wishes of both parents and child where treatment is vital to the child's welfare.

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.

14. The Information Commissioner offers guidance as to the meaning of the phrase 'disproportionate effort'. See www.informationcommissioner.gov.uk.
15. Serious crime, as defined by the GMC (General Medical Council) 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).
16. AIDS (Control) Act 1987; National Health Service (Venereal Diseases) Regulations 1974; National Health Service Act 1977; National Health Service Trusts (Venereal Diseases) Directions 1991
17. Human Fertilisation and Embryology Act 1990: ss 31 & 33; Human Fertilisation and Embryology (Disclosure of Information) Act 1992

Other Formats

This report is available in large print, or other formats, if required.

Please contact:

Social Services Inspectorate for Wales

Cathays Park

Cardiff

Telephone: 029 2082 5655

E-mail: ssiw@wales.gsi.gov.uk