



Department of
**Health, Social Services
and Public Safety**

www.dhsspsni.gov.uk

AN ROINN

**Sláinte, Seirbhísí Sóisialta
agus Sábháilteachta Poiblí**

MÁNYSTRE O

**Poustie, Resydènter Heisin
an Fowk Siccar**

Code of Practice on Protecting the Confidentiality of Service User Information

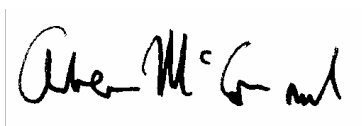
January 2009

FOREWORD

All users of our health and social care services have the expectation that any personal information they provide will be treated as confidential. However, the use and sharing of personal information forms an essential part of the provision of health and social care, benefitting individual users of the services and often necessary for the effective functioning of health and social services. Staff working within health and social services have an ethical and legal obligation to protect the information entrusted to them by users of the services.

This Code of Practice on confidentiality has been developed by the Privacy Advisory Committee established by the Department of Health, Social Services and Public Safety. The purpose of the Code of Practice is to provide support and guidance, for all those involved in health and social care, concerning decisions about the protection, use and disclosure of service user information. It follows a comprehensive round of public consultation during 2007 which included the Health and Social Services Councils, Professional Regulatory Bodies, the Information Commissioner's Office, the Digital Information Policy Branch of Department of Health in England.

The Code provides an invaluable reference point for everyone working within health and social care in Northern Ireland on all matters related to privacy and confidentiality and I commend it to you.

A handwritten signature in black ink, appearing to read 'Andrew McCormick', enclosed in a thin black rectangular border.

Andrew McCormick
Permanent Secretary
Department of Health Social Services and Public Safety

January 2009

Contents

Foreword

Preface

1. Introduction
2. Service User Information
 - Keeping service users informed
 - Consent
 - Supporting the service user's right of access to their records
 - Respecting privacy in seeking and in using service user information
 - Maintaining information in a form which protects the identity of the service user
 - Maintaining the confidentiality of information after a service user's death
 - Managing information and records
3. The purpose of any anticipated use or disclosure of person identifiable service user information
 - (A) The use and disclosure of person identifiable information for the direct care of that service user
 - Consent in the provision of direct care
 - Emergency Situations
 - Review of care, including clinical audit
 - Multidisciplinary teams and inter-agency working
 - Sharing information with informal carers
 - Dual roles
 - (B) The use and disclosure of person identifiable information for purposes of health and social care not directly related to care of that service user (secondary uses)
 - Consent and Secondary Uses
 - Uses and Disclosures for Secondary Purposes
 - (C) Use and disclosure of person identifiable information for other purposes
 - Consent and the use and disclosure of information for other purposes
 - Obligations to Disclose

Discretionary Disclosures in the Public Interest
A flow diagram to assist good practice

4. Decision making about information use or disclosure relating to adults lacking capacity
 - Determining 'best interests'
 - Carers and Advocates

5. Decision-making about the personal information of children
 - Disclosures in the Public Interest
 - Disclosures when a child or young person lacks the capacity to consent
 - Access to medical records by children, young people and their parents
 - Child protection

Appendix 1: The Ethics and Law of Confidentiality

Appendix 2: The Principal Northern Ireland Laws Relating to Confidentiality and Disclosure

Appendix 3: Membership of Privacy Advisory Committee (Northern Ireland)

Appendix 4: Further Information and Guidance

Preface

The use and sharing of service user personal information forms an essential part of the provision of health and social care, benefiting individual service users, often necessary for the effective functioning of health and social services and often necessary in the public interest. The essential nature of such uses however needs to be set alongside the expectations service users have that all personal information will be kept confidential. All health and social care staff therefore have strong ethical and legal obligations to protect service user information (Appendices 1 and 2).

The relationship between health and social care staff and the service user should be one of fidelity or trust. Service users have a tacit understanding that private information will not be used or disclosed without their awareness and consent.

The nature of the obligation to protect confidentiality can be expressed in terms of three core ethical principles which underpin the law:

- individuals have a fundamental right to the confidentiality and privacy of information related to their health and social care;
- individuals have a right to control access to and the disclosure of their own health and social care information by giving, withholding or withdrawing consent;
- for any disclosure of confidential information health and social care staff should have regard to its necessity, proportionality and any risks attached to it.

Each service user's right to privacy and staff's duty of confidentiality apply regardless of the form in which information is held or communicated, for example electronic, paper, photographic, biological.

Particular care is needed on the part of health and social care staff to ensure that the right to privacy of vulnerable people – specifically adults with incapacity and children – is respected and the duty of confidentiality owed to them is fulfilled.

The Code of Practice was equality screened in accordance with Section 75 of the Northern Ireland Act 1998 which requires the Department to “have due regard” to the need to promote equality of opportunity across nine categories and also to “have regard” to the desirability of promoting good relations. Equality screening is carried out to determine if a policy or practice is likely to have a significant impact on equality of opportunity and should therefore be

subjected to an equality impact assessment (EQIA). The Department concluded that an EQIA was not required because the Code of Practice will affect all those accessing and working in health and social services. This is a positive initiative which will raise the profile of confidentiality, making staff more aware of the need to keep information confidential and supporting them in making sound decisions about when and how information can and should be shared and, at the same time, providing reassurance to service users and making them more aware of their rights in relation to their personal information.

The Code of Practice is principally concerned with identifiable service user information. Uses or disclosures of such information are only justified where either:

- service user consent has been given, or
- there is a statutory requirement, or
- the balance of public and private interest favours disclosure. In such situations there must be substantial public interest favouring disclosure which outweighs both the private interests of the individual and the public interest in safeguarding confidentiality.

In Northern Ireland there is no equivalent to section 251 of the National Health Service Act 2006¹, which allows the setting aside of the common law duty of confidentiality for such essential health and social care purposes. The need for statutory provision for health and social care information governance including the uses and disclosures of confidential identifiable service user information is presently being considered by the Department.

The Privacy Advisory Committee (N Ireland) (Appendix 3) as part of its role will support Personal Data Guardians and the Regional Quality Improvement Authority in ensuring that the information governance standards reflected by this confidentiality code of practice are maintained by all organisations providing health and social care.

¹2006 c.41

CHAPTER 1. Introduction

- 1.1 The aim of this Code of Practice is to support staff in making good decisions about the protection, use and disclosure of service user information. It provides practical guidance to assist decision-making with respect to service user information and a method for considering decisions.
- 1.2 The Code of Practice should be the reference point for all staff and any questions which it does not answer should be addressed to the relevant Personal Data Guardian or member of staff responsible for data protection. Difficult decisions will always remain to be made in situations which cannot be addressed in detail in a Code of Practice. Data protection law, human rights law and the common law of confidentiality are all complex and can interact in highly complex ways in particular situations. Occasionally it may be necessary to ask for a professional legal opinion.
- 1.3 This Code of Practice replaces earlier guidance “The Protection and Use of Patient and Client Information” (June 1999). It should not be taken as a complete statement of the law and legal advice should be sought when necessary. Further ethical and legal developments, changes in policy, or relevant new guidance may occur after this Code of Practice has been issued. Health and social care staff should endeavour to keep themselves informed of any developments which may be relevant to their practice.
- 1.4 Issues in relation to information handling are considered in Chapter 2. In Chapter 3 the Duty of Confidentiality is considered in relation to the three main purposes of any anticipated use – the use and disclosure of information for the direct care of that service user; the use and disclosure of information for purposes of health and social care not directly related to the care of that service user (Secondary Uses); and the uses and disclosure of information for other purposes. Particular consideration is given to good practice in making decisions about information use or disclosure with adults lacking capacity (Chapter 4) and in relation to the personal information of children (Chapter 5).
- 1.5 New and changing issues in relation to confidentiality and privacy are constantly arising. This Code of Practice must of necessity be a living document and will therefore require regular review and updating.

CHAPTER 2. Service User Information

- 2.1 Health and social care professionals have an obligation to keep records and this should be made clear to service users and any concerns they have about records should be addressed.

Keeping service users informed

- 2.2 Modern health and social care services often involve sharing information between staff to provide optimal care and treatment, but the extent of and their control over such sharing is not always known to service users. Service users must be kept informed in an accessible manner (including making use of appropriate communication supports) about the uses and disclosures of their information. It is important that service users are informed of the limitations of confidentiality, both in terms of any relevant statutory obligations to disclose confidential information and of the duty of health and social care staff to disclose information in the public interest (see 3.19–3.27).
- 2.3 Service users must also be informed of the circumstances in which they can give, withhold or withdraw consent to the use of their information.
- 2.4 In general, service users should be informed of:
- what kinds of information are being recorded and retained;
 - the purposes for which the information is being recorded and retained;
 - what protections are in place to ensure non-disclosure of their information;
 - what kinds of information sharing will usually occur;
 - the choices available to them about how their information may be used and disclosed;
 - their rights to access and where necessary to correct the information held about them within health and/or social care records.
- 2.5 Service users should be told how information will be used before they are asked to provide it and should be given an opportunity to discuss such uses. It should be made clear to service users that they may object to specific secondary uses of identifiable service user information (see 2.7).

Consent

- 2.6 Consent is the means by which the service user can exercise control over the dissemination of their confidential information. Use or disclosure of person identifiable information is normally justified by the consent of the service user. For most uses of information, consent may be withdrawn.
- 2.7 If the service user refuses to consent to disclosure of personal information, the information cannot be disclosed, unless, exceptionally, a justification other than consent exists. Staff should discuss with the service user why he/she thinks that disclosure is in the service user's best interests and the potential disadvantages that may arise. Unless there is an overriding public interest justification, information should not be disclosed on a "best interests" basis where an adult with capacity refuses to consent to disclosure.
- 2.8 Disclosure in a service user's best interest would usually be justified:
- where an adult is incapable of giving or withholding consent and you believe they are a victim of neglect or of emotional or physical abuse, or at risk of suicide
 - where without disclosure you would not be acting in the overall best interests of a child and where it is impractical or inappropriate to obtain consent from the person with parental responsibility.

Supporting the service user's right of access to their records

- 2.9 One of the key means by which service users exercise their rights is through their general right of access to their health and social care records.
- 2.10 Information in the record about third parties (other than relevant health professionals) should not in general be disclosed without the consent of the third party. Information should not be disclosed where its release may cause serious harm to the physical or mental health or condition of the service user or any other person.

Respecting privacy in seeking and in using service user information

- 2.11 A lack of respect for the privacy of service users may be shown not only in how information is used or disclosed, but also in the manner in which it is initially obtained. Service users should not be asked questions which may require their revealing of private, sensitive or confidential

information in a way which will be overheard or inadvertently accessible to others. Respect for privacy requires a reasonable caution in soliciting the information necessary for the care of service users. Service users must not be deceived or misled as to the purpose or purposes for which their information is sought.

- 2.12 Private information should in general only be requested from or provided to service users in an appropriate environment, for example, where others cannot overhear. What exactly is appropriate will depend on the nature of the information likely to be offered by/to the service user. Reasonable steps should be taken to ensure the privacy of the service user in a proportionate manner. Any means of communication of private information (for example, telephone or email) should be sufficiently secure to ensure the privacy of the service user.
- 2.13 If a member of staff is seeking information from another member of staff, then it should only be sought from someone with legitimate access to that information and with the authority to disclose it. The identity of any person requesting information, including someone claiming to be a member of health and social care staff, should be checked when necessary.
- 2.14 Gossiping is clearly an improper use of confidential service user information, but care must also be taken in discussing cases in public places. Cases may need to be discussed with colleagues (for example, to gain advice or share experience), but the service user should not be identified unnecessarily and care must be taken that others do not overhear these conversations.

Maintaining information in a form which protects the identity of the service user

- 2.15 The highest standards of security should apply to service user information. Staff should reasonably satisfy themselves that information they disclose will be kept in a manner which is in keeping with such standards. Unless requested by the service user, the release of service user information is the responsibility of the data controller. This is normally the holding organization. In situations of uncertainty, check with the Personal Data Guardian.
- 2.16 Many secondary uses of service user information do not need to identify service users. In such situations the information should be held

in the form which minimizes any risk of identification. Anonymisation and pseudonymisation are key means for protecting the rights of service users. Where appropriate all organisations should aim to anonymise or pseudonymise information.

- 2.17 It is common to refer to information as ‘anonymised’ when it is not immediately apparent to whom the information refers. However, for the purposes of data protection, a much stricter definition of ‘anonymous’ is provided by law. For personal data to have been rendered anonymous it must no longer be possible for anyone to identify the person who is the subject of the data directly (that is, from the data itself) or indirectly (that is, from the data itself in conjunction with other data or means that are ‘reasonably likely to be used’, such as an identification number or to one or more factors specific to the subject's physical, physiological, mental, economic, cultural or social identity).
- 2.18 ‘Pseudonymised information’ is like anonymised information in that in the possession of the holder it cannot be used by the holder to identify an individual. However it differs in that the original provider of the information, who may even belong to the same organisation, 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.
- 2.19 Where full anonymisation is impracticable, the information holder will need to consider the potential risks to service user confidentiality before sharing the information in a pseudonymised form.

Maintaining the confidentiality of information after a service user's death

- 2.20 The confidential nature of a service user's information and the ethical obligation on health and social care staff to respect that confidentiality remain after the death of that service user. However, just as in life, the duty to maintain confidentiality after death is not absolute, but is subject to ethical and legal limitations. Even though the service user can no longer be harmed, there is still a public interest in the maintenance of confidentiality after death. Disclosure of information after the death of a service user might be an infringement of the right to private life of people associated with the service user.

2.21 A competent service user can give or withhold consent to disclosure before their death and such wishes should be respected as they would in other circumstances. In particular, where a competent service user has made an explicit request before his or her death that their confidence be maintained, then the service user's request should normally be respected.

Managing Information and Records

2.22 Good records management standards and practices underpin respect for the privacy of service user information. Specifically, it is essential that case files and associated records (such as images or notes) are stored securely, that they can be located at any time and that they are disposed of in a way and at a time consistent with the regional guidelines and the organisation's disposal schedule.

2.23 Using an electronic record can provide greater quality and security of health and social care information than the traditional forms of documentation. However, they also have the potential to make a service user's information more readily available to a wider range of people. Electronic records therefore must be appropriately protected.

CHAPTER 3. The purpose of any anticipated use or disclosure of person identifiable service user information

3.1 A key means for the protection of service user information is the requirement for a clear and unambiguous purpose for any contemplated use or disclosure. Clarity about the purpose of any contemplated use or disclosure is a key feature of ethics, human rights law, data protection law and the common law of confidentiality. Only the minimum information consistent with that purpose should be used or disclosed.

3.2 The particular purpose of any contemplated use or disclosure of service user information will be one of the following:

(A) use and disclosure of personal identifiable information for the *direct care* of that service user;

(B) use and disclosure of personal identifiable information for purposes of health and social care *not directly related to the care of* that service user (secondary uses);

(C) uses and disclosures of personal identifiable information for purposes other than A or B.

It is important to note that a use or disclosure for any of these purposes may have several possible justifications. In particular instances use or disclosure might be justified on the basis of the consent of the service user, a statutory obligation or in the overriding public interest for any of these purposes.

3.3 To facilitate good practice a flow diagram of the decision-making process is provided at the end of this chapter. This draws attention to the most relevant considerations for each purpose.

(A) Use and disclosure of personal identifiable information for the direct care of that service user

Consent in the provision of direct care

3.4 As with any other intervention forming part of the provision of direct care for a service user, their consent occupies a pivotal role in legitimising the uses and disclosures of their information. Service users must be informed in a manner appropriate to their communication needs of what information sharing is necessary for their care and the likely extent of

the sharing for a particular episode of care. Provided they are adequately informed in this way (see Ch. 2), express consent is not necessary and the consent of the service user to the disclosure of information necessary for their care may be inferred from their acceptance of that care.

- 3.5 The co-operation of a service user alone is not a sufficient basis on which to infer their consent to the use or disclosure of their information. It must be clearly understood by the service user that the disclosure will take place unless they dissent and it must also be clear to the service user that they can dissent, though the implications for their care should be explained to them). If there is doubt that these conditions are fulfilled express consent should be sought from the service user.

Emergency Situations

- 3.6 In emergency situations it may be impossible to keep a service user properly informed and to gain their valid consent. In such situations, uses or disclosures may be made, but only the minimum necessary information should be used or disclosed to deal with the emergency situation. Reasonable care should be taken not to override any relevant legally binding wishes of the service user which have been expressed in advance of the situation arising. As soon as possible, the service user should be told what information has been disclosed and their consent sought for any necessary further disclosures.

Review of care

- 3.7 Review of care, including clinical audit and case review, carried out by members of the care team and those supporting them, is for the purpose of improving the direct care of that service user. Such purposes have sufficient connection with that direct care for the sharing of information during the review of care to be justified on the basis of implied consent.

Multidisciplinary teams and inter-agency working

- 3.8 When health and social care staff legitimately disclose service user information for the care of that person in a multidisciplinary team or in inter-agency working, such disclosure should take place on a clear basis of agreed protocols for information sharing.

- 3.9 Whilst the underlying principles are the same, health and social care staff may have different criteria and thresholds for the disclosure of confidential information, for example in relation to public safety. All staff, insofar as it is necessary for their work, have a responsibility to familiarise themselves with such differences and moderate disclosures accordingly.
- 3.10 It is common practice in many areas of health and social care provision to involve outside agencies in providing services. This inevitably involves discussions about service users at various points in their care. Issues about sharing information may arise in the context of verbal or written reports, or attendance at case conferences. Where it is planned to involve staff from other agencies this should first be discussed with the service user and their explicit consent should be sought. The particular purpose of involving the other agency should be clarified along with the purpose of the proposed information sharing. When other agencies request information about service users, health and social care staff should seek the consent of the service user.

Sharing information with informal carers

- 3.11 Family members and other persons who are providing informal care for a service user have an understandable need for information about their care problems and management. Such knowledge may benefit both the service user and the carer by, for example, creating a better understanding of the needs of the service user and promoting more appropriate responses to them. However, the fact that such information sharing may be beneficial does not diminish the duty of confidentiality owed to the service user. In situations of ongoing need for care and support, the potential benefits of information sharing with their informal carers should be discussed with the service user.
- 3.12 A carer may share information in confidence for the benefit of improved care for the service user and particularly on the understanding that it will not be disclosed to the service user that such information sharing has taken place. The interests of carers should be protected and in general their right to privacy and confidentiality should also be respected.

Dual roles

- 3.13 Health and social care staff should avoid situations with dual responsibilities and obligations to the same service user wherever

possible. For example where a doctor may find themselves being a person's General Practitioner and an Occupational Health Physician where the person is an employee. Where a staff member has dual responsibilities it is important that they explain to the service user at the start of any consultation or assessment on whose behalf they are seeing them and the purpose of the consultation or assessment. It should also be made clear to the service user the extent to which information given will not be treated as confidential. Nevertheless the general and professional obligations to maintain confidentiality remain.

(B) The use of personal identifiable information for purposes of health and social care not directly related to care of that service user (secondary uses)

3.14 Some uses and disclosures of service user information are for purposes of health and social care not directly related to the care of an individual service user. Many uses of service user information are increasingly required for evidence based practice and for a rational approach to health and social care service provision - for which uses there is a public interest. The following are examples of such secondary uses: planning; financial management; commissioning; risk management; investigating complaints; auditing accounts; teaching; health and social care research; public health monitoring; registries; infectious disease reporting.

Consent and secondary uses

3.15 From a consent perspective, a clear distinction must be drawn between disclosures which are necessary for the purpose of the care of the service user and disclosures which are for maintaining or improving the general functioning of health and social care services.

3.16 While the co-operation of a service user can provide a basis for inferring their consent to the use and disclosure of information required for their care, there is no behaviour which clearly implies consent to other uses and disclosures. Therefore when the purpose of a use or disclosure relates to health and social care, but is not directly for the care of that service user, the express consent of that service user is usually required. The possible exceptions to this requirement for consent are where a statute, court or tribunal imposes a requirement to disclosure or there is an overriding public interest in the use or disclosure (see 3.19).

Uses and Disclosures for Secondary Purposes

3.17 The following principles for good practice should be followed when considering use and disclosure of information for secondary purposes:

- All organisations seeking to use confidential service user information should provide information to service users describing the information they want to use, why they need it and the choices they may have.
- Where an organisation has a direct relationship with a service user then it should be aiming to implement procedures for obtaining the express consent of the service user.
- Where consent is being sought this should be by health and social care staff who have a direct relationship with the individual service user.
- 'Third Party' organisations seeking information other than for direct care should be seeking anonymised or pseudonymised data.
- Any proposed use must be for some clear general good or for the clear benefit of service users.
- Organisations should not collect secondary data on service users who opt out by specifically refusing consent.
- Service users and/or service user organisations should be involved in the development of any project involving the use of confidential information and the associated policies.
- To assist the process of pseudonymisation the Health and Care Number of Service Users should be used wherever possible.

3.18 Situations arise where the consent of service users cannot practicably be obtained for use or disclosure yet there are clearly public health and social care interests. Examples include disease registries, administrative and financial monitoring, financial inspections - including probity checking to provide assurance on the level of service provision. The Department is presently giving consideration to the introduction of legal support for non-consented use of service user identifiable information for essential health and social care purposes.

(C) Use and disclosure of personal identifiable information for other purposes

3.19 It is sometimes both legally and ethically acceptable to use or disclose service user information for purposes which are neither for the direct care of that service user nor for a secondary health and social care purpose. Examples of such purposes include: prevention of serious harm to third parties; child protection; protecting vulnerable adults; prevention of terrorism; prevention, detection or prosecution of a serious crime; misuse of controlled drugs; investigation of serious professional misconduct..

Consent and the use and disclosure of information for other purposes

3.20 Consent is not required where there is a statutory obligation to disclose or a discretionary disclosure is justified in the public interest. However, it may be necessary to seek consent for a disclosure where the public interest served does not clearly override the public interest in maintaining confidentiality. In other circumstances it might still be appropriate to discuss disclosure with the service user in order to protect the relationship with them, even though the disclosure does not need their consent to be justified.

Obligations to Disclose

3.21 Where a statute, court or tribunal imposes a requirement to disclose information, care should be taken only to disclose the information required to comply with and fulfil the purpose of the law (see Appendix 2). If you have reason to believe that complying with a statutory obligation to disclose information would cause serious harm to the service user or another person, you should seek legal advice.

Discretionary Disclosures in the Public Interest

3.22 In all cases of discretionary disclosure in the public interest, there is no legal obligation to disclose, but whether or not disclosure can be justified depends on balancing the interests that are in conflict in each case, for example protecting a third party from serious harm. It needs to be borne in mind that every disclosure is an interference with the service user's right to privacy, while the benefits of disclosure will often be less certain. While a balancing of the service user's right to privacy

against other rights and interests is always difficult, it is usually more easily performed where the conflict is with rights of identifiable third parties, such as in child protection, than where there is a conflict with a more diffuse public interest such as national security or public health. It is not sufficient that such disclosure might serve the protection of such an overriding public interest; rather the test is one of strict necessity in the specific circumstances of each case.

- 3.23 In situations involving disclosure to protect overriding rights of third parties, each case must be considered on its merits. The test is whether the release of information to protect the interests of a third party exceptionally prevails over the duty of confidence owed to the service user and the public interest in a confidential health and social care service. In performing the balancing exercise it is important to remember that there is a substantial public interest in the maintenance of confidentiality in health and social care services and not to construe the balance as being between the rights of an individual alone against the public interest.
- 3.24 Health and social care staff could be found to be negligent if a disclosure was not made but a public interest justification could clearly be made and harm resulted.
- 3.25 Factors to consider when reaching a decision to disclose are:
- the importance of the interest that is at risk without disclosure, for example disclosure might be more easily justified where the life or integrity (physical or psychological) of a third party is at risk;
 - the likelihood of the harm occurring in the individual case, that is, disclosure might be justified where there is a high likelihood of harm to the life of another, but not necessarily justified where there is a low likelihood of harm;
 - the imminence of the harm, that is, disclosure might be justified where protection of the third party requires immediate action, but not where there is no more than a possibility that at some future point the service user might pose a threat to another;
 - the existence of an appropriate person to whom disclosure can be considered;
 - the necessity of the disclosure to avert the harm, that is, that there is no reasonable possibility of averting the harm without disclosure;
 - the likelihood that disclosure can avert the harm, which requires that the health or social care staff member be satisfied that the harm

to the third party or to the public interest is sufficiently likely to be averted by disclosure.

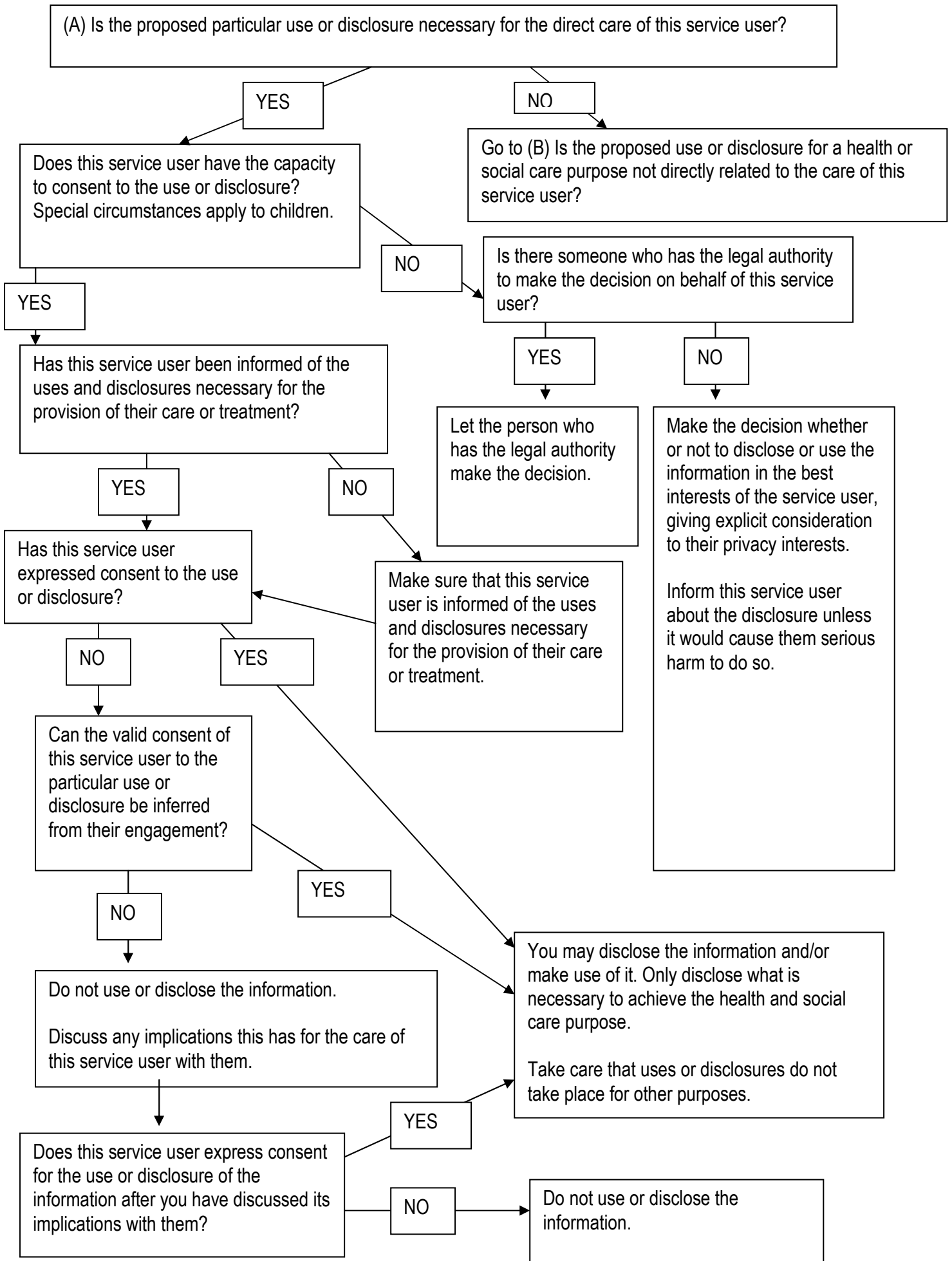
- 3.26 In all instances where judgment is involved, health and social care staff are urged to discuss the case with colleagues without revealing identifiable details of the service user and, if necessary, to seek legal or other specialist advice. It may be more appropriate in certain situations for the decision to be made by a middle or senior manager. When a decision has been reached that disclosure is justified in a particular situation, there are requirements for how that disclosure should best be made. Most situations where decisions to disclose are reached require good communication with and support for service users whose confidentiality is to be breached. The member of staff should record in the health record or social care record details of all conversations, meetings and appointments involved in the decision to disclose or not to disclose such information.
- 3.27 Once a decision to disclose has been reached the usual procedure would be as follows:
- an explanation of the reasons for sharing information should be given in writing to the service user and/or people with responsibility for them such as parents;
 - the responsible member of staff should encourage the service user (and/or where appropriate, their legal representative) to inform the relevant authority (for example, police or social services). If the service user or legal representative agrees, the member of staff will require confirmation from the authority that such disclosure has been made;
 - if the service user or their legal representative refuses to act, the responsible member of staff should then tell them that he or she intends to disclose the information to the relevant authority or person. He or she should then inform the authority, disclosing only relevant information and make available to the service user and/or their legal representative the information that he or she has released; and
 - health and social care staff who decide to disclose confidential information (with or without prior informing of the service user and/or their legal representative) should be prepared to explain and justify their decision to the authority if called upon to do so.

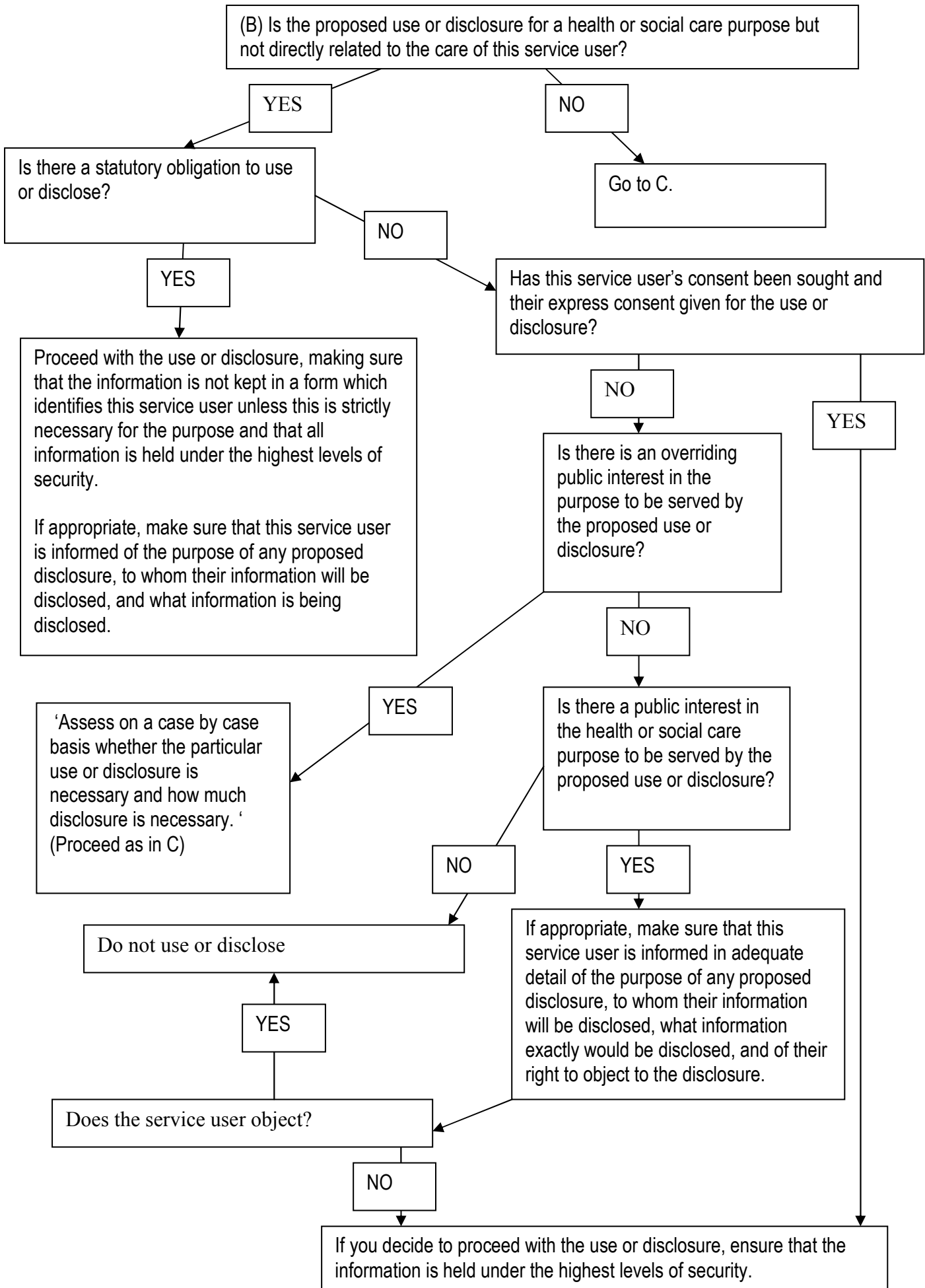
Exceptions to this normal procedure could be where informing the subject in advance would prevent achieving the justified aim of the

disclosure and where doing so would put the safety of the member of staff or another person at risk.

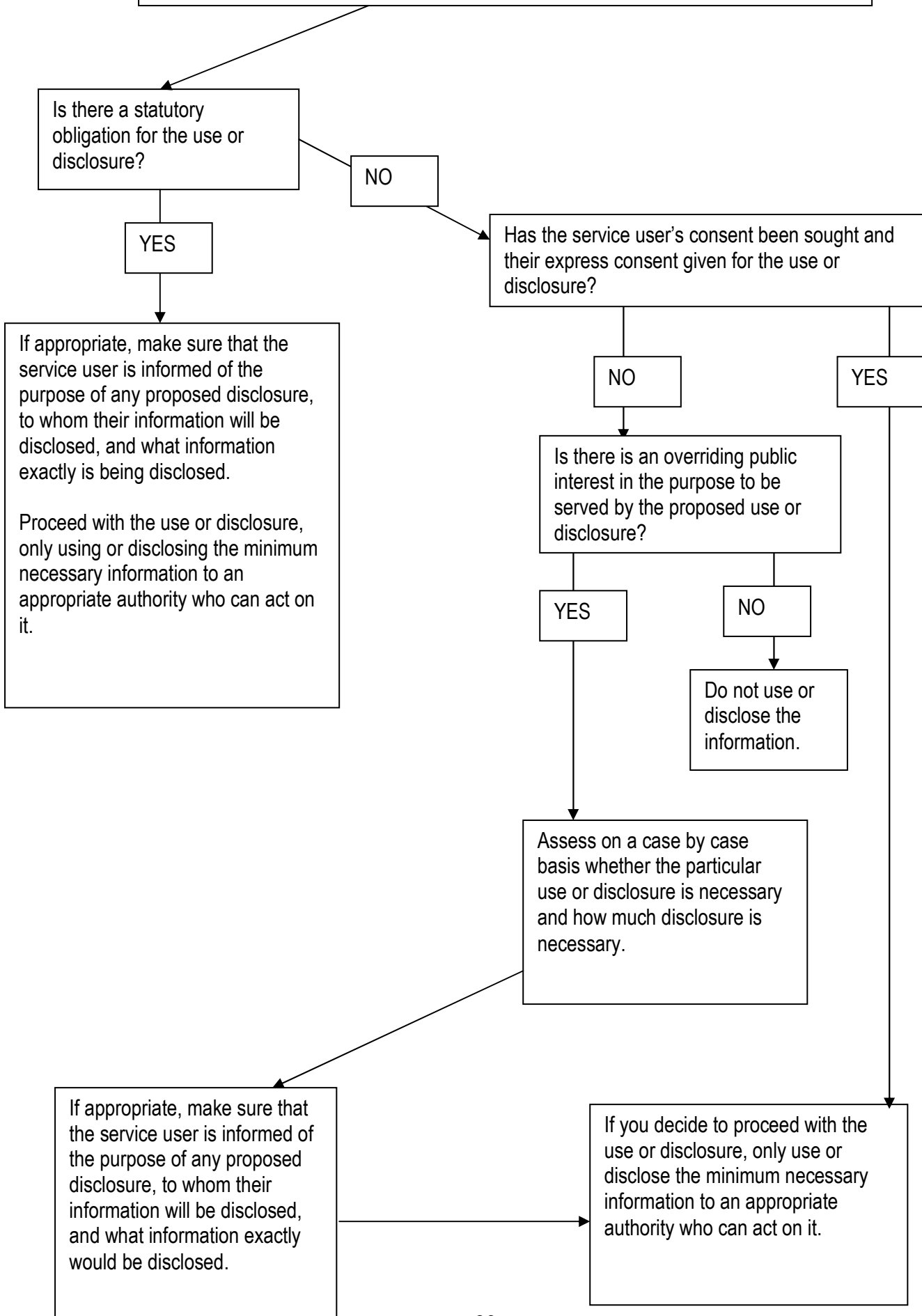
A Flow Diagram to Assist Good Practice

- 3.28 The following flow chart provide a simple tool to direct your attention to the key considerations in making good decisions about the use and disclosure of personal identifiable service user information. It must be used in conjunction with the body of this Code of Practice and it contains references to the particularly relevant paragraphs in brackets.
- 3.29 The chart falls into three sections which correspond to the distinction in the text between the three kinds of purpose of any proposed use or disclosure. These three kinds of purposes are:
- (A) use and disclosure of personal identifiable information for the direct care of that service user;
 - (B) use and disclosure of personal identifiable information for purposes of health and social care not directly related to care of that service user;
 - (C) use and disclosure of personal identifiable information for other purposes.
- 3.30 Any proposed use or disclosure will necessarily fall under one of these three general types of purpose. To use the decision tree begin by considering A and where appropriate proceed to B and then to C as indicated on the decision tree.





(C) The proposed use or disclosure is for other purposes



CHAPTER 4. Decision making about information use or disclosure relating to adults lacking capacity

- 4.1 All service users have the right to the privacy of their health and social care information and this right is in no way diminished because a service user lacks decision making capacity in some respect. In such circumstances decisions should in general be made in the best interests of the service user. The protection of the privacy interests of service users who lack capacity is in general in their best interests.
- 4.2 As with other service users, there is the possibility of a statute or a public interest which overrides the public interest in maintaining the confidentiality of service users who lack capacity.

Determining 'Best Interests'

- 4.3 In determining the best interests of a service user who lacks capacity, particular consideration must be given as to how the opinions of others can be gained without inappropriately disclosing confidential information to them. Disclosing information to others to seek their opinion on the best interests of the service user may not itself be in the best interests of the service user.
- 4.4 An adult has the capacity to give or withhold consent to the use or disclosure of their information if he or she can:
- understand and retain the information relevant to the decision in question;
 - believe that information;
 - weigh that information in the balance to arrive at a choice.
- 4.5 It is important that capacity is assessed for particular decisions at particular times and where possible decisions should be postponed until a service user with fluctuating capacity is able to make the decision him or herself. In general, a person with the capacity to make decisions about privacy issues should be able to exhibit all of the following:
- show understanding of the idea of disclosure of confidential information about themselves;
 - show understanding of the possible implications of agreeing to the disclosure of information or of refusing it;
 - retain the information sufficiently to come to a decision;
 - believe the relevant information;
 - come to a decision;

- communicate their decision.

4.6 Where a service user lacks the capacity to make a particular decision about the use or disclosure of their information, then any use or disclosure must be strictly necessary and any decision made must be in the best interests of that service user. In determining the best interests of a service user when there is a need to make a decision regarding the use or disclosure of their information, the following should be considered:

- the service user's own wishes and values (where these can be ascertained), including any advance statement;
- the effectiveness of the use or disclosure, particularly in relation to other options;
- where there is more than one option, which option is least restrictive of the service user's future choices;
- the likelihood and extent of any benefit to the service user if the use or disclosure is made;
- the views of the parents, if the service user is a child;
- the views of people close to the service user, especially close relatives, partners, carers or proxy decision makers about what the service user is likely to see as beneficial; and
- any knowledge of the service user's religious, cultural and other non-medical views that might have an impact on the service user's wishes.

Carers and Advocates

4.7 In some circumstances it may be appropriate to consult carers or advocates in considering what is in the best interests of a service user who lacks capacity. It is important to be clear on the limits of the ability of carers and advocates to legally represent the interests of the service user and the need to maintain the confidentiality of the service user with respect to them.

CHAPTER 5. Decision-Making about the personal information of children¹

- 5.1 Children have the same rights to privacy as all others and there is the same duty of confidentiality to them as there is to adults.
- 5.2 Children may have particular needs when it comes to the provision of information about uses and disclosures. It is important that the rights of children and young people are equally respected in this area and this may mean using different methods of providing information to those used for adults.
- 5.3 Sharing information with the right people can help to protect children and young people from harm and ensure that they get the help they need. It can also reduce the number of times they are asked the same questions by different professionals. Asking for consent to share relevant information shows respect and involves children in decisions about their care.
- 5.4 If children and young people are able to take part in decision-making then they should be provided with an explanation of why it is proposed to use or disclose information and their consent sought, including consent to talk to parents and others involved in their care or treatment.
- 5.5 Personal information about a child should not be shared more widely than is strictly necessary, for example, in meetings with other professionals such as teachers.
- 5.6 Information required by statute, court order or a tribunal must be disclosed.

Disclosures in the Public Interest

- 5.7 Information should be disclosed if it is necessary to protect the child or someone else from risk of death or serious harm. Such cases may arise, for example, if:
- a child or young person is at risk of neglect or sexual, physical or emotional abuse;
 - the information would help in the prevention, detection or prosecution of serious crime, usually crime against the person;²

¹ This section of the Code of Practice has been based on the GMC's "0-18 years: guidance for all doctors" (2007).

- a child or young person is involved in behaviour that might put them or others at risk of serious harm, such as serious addiction, self-harm or joy-riding.

If disclosure is considered to be justified, disclose the information promptly to an appropriate person or authority and record your discussions and reasons. If disclosure is not justified, record your reasons for not disclosing.

Disclosures when a child or young person lacks the capacity to consent

5.8 Occasionally, children who lack the capacity to consent might disclose information on the understanding that their parents are not informed. Staff should try to persuade the child to involve a parent in such circumstances. If they refuse and it is considered necessary in the child's best interests for the information to be shared (for example, to enable a parent to make an important decision, or to provide proper care for the child), information may be disclosed to parents or appropriate authorities. Discussions and reasons for sharing the information should be recorded in the case notes.

Access to medical records by children, young people and their parents

5.9 Young people with capacity have the legal right to access their own health records and can allow or prevent access by others, including their parents. Children should usually be supported in accessing their own health records.

5.10 If a child or young person consents, or lacks capacity, and it does not go against the child's best interests, parents should be given access to their child's medical records. If the records contain information given by the child or young person in confidence the information should not normally be disclosed without their consent.

Child protection

5.11 There can be conflict between child protection and confidentiality. Both are extremely important in safeguarding the welfare of children. Health and social care staff play a crucial role in protecting children from abuse and neglect. Staff may be told or

notice things that others may not and may have access to confidential information that causes them to have concern for the safety or well-being of children.

- 5.12 Confidentiality is important and information sharing should be proportionate to the risk of harm. Some limited information may be shared, with consent if possible, in order to decide if there is a risk that would justify further disclosures. Disclosing information is justified in raising a concern, even if the concern turns out to be groundless, if it is done honestly, promptly, on the basis of reasonable belief, and through the appropriate channels.
- 5.13 Children, young people and parents may not want you to disclose information about them if they think they will be denied help, blamed or made to feel ashamed. They might have had bad experiences or fear contact with the police or social services. They should be assisted in understanding the importance and benefits of information sharing.
- 5.14 The protection of children from harm is in the public interest and this is what can legally justify breaching confidentiality in certain situations. Sharing relevant information with an appropriate person or authority should not be delayed if this would increase the risk of harm to the child or young person or to other children or young people.

Appendix 1: The Ethics and Law of Confidentiality

Ethical standards for the protection of service user information may be higher than legal standards. Even where legal obligations are satisfied, a particular use or disclosure may not necessarily be ethical. Where ethical standards require greater protection for service user confidentiality than legal standards, then health and social care staff should follow professional ethical obligations.

It is important to note that disciplinary consequences may follow from a breach of ethical standards set by regulatory authorities.

Ethical and legal protections apply both to any *disclosure* of service user information and to any *use* of it.

Ethical obligations to protect service user privacy

The nature of the obligation to protect confidentiality can be expressed in terms of three core ethical principles which underpin the law.

- Individuals have a fundamental right to the confidentiality and privacy of information related to their health and social care.
- Individuals have a right to control access to and disclosure of their own health and social care information by giving, withholding or withdrawing consent.
- For any disclosure of confidential information health and social care staff should have regard to its necessity, proportionality and any risks attached to it.

Just as the service user has a right to self-determination in various other health and social care matters, it is in general the service user's decision as to who should have access to personal health and social care information and the purpose for which it may be used.

One reason for respecting confidences in health and social care is that doing so enables service users to disclose sensitive information that health and social care staff need to provide treatment or care. Without an assurance that confidentiality will be maintained, service users might be less willing to disclose information, resulting in obstacles to their effective care and negative effects for their health and for public health.

None of the ethical arguments stated above lead to the conclusion that the ethical duty of confidentiality is absolute. The confidentiality requirement exists within a wider social context in which members of staff have other duties which may conflict with their duty of confidentiality. In particular, they may have other ethical duties to disclose confidential information, without

consent, if serious dangers are present for third parties or for the service user and where they judge that the disclosure of that information is likely to significantly reduce or eliminate the danger. In assessing such risks and whether they outweigh the duty of confidentiality both the probability of the harm and its magnitude need to be considered. The ethical duty to disclose to prevent harm is generally greater when both the probability and the seriousness of harm to a third party or the service user are high.

Legal obligations to protect service user privacy

Legal obligations to protect the privacy of service users stem from three main sources:

- Common law of confidentiality
- Data Protection Law
- Human Rights law

The requirements of the legal standards may differ. It is important to note that meeting the obligations of one source does not guarantee that the obligations under the others are being met. For example, the consent of a service user for a particular use may not be required by data protection law, but may be a common law requirement.

The interaction of laws relating to privacy and confidentiality with other laws should be considered when necessary. In particular, additional legal requirements may apply when the service user is a child or young person or an adult who lacks capacity.

The pressures from outside health and social care for health and social care information can change in changing social, economic and political climates. It is important that the wishes and interests of service users remain at the heart of health and social care. The limits on policy and legislation set by human rights law are important protections for service users and the duty to act in keeping with their human rights obligations is a highly important duty of all health and social care staff.

Appendix 2:

The Principal Northern Ireland's laws relating to confidentiality and disclosure

GENERAL LAWS

The common law

The key principles of the law of confidentiality are contained in the common law, that is, in the decisions of judges in particular cases. A duty of confidence arises when confidential information comes to the knowledge of a person (the confidant) in circumstances where that person has notice, or is held to have agreed, that the information is confidential, with the effect that it would be just in all circumstances that he or she should be precluded from disclosing the information to others. The relationship between a health or social care provider and a user of those services constitutes such a circumstance. In the event of a breach of this duty of confidence, legal action may follow, including claims for an injunction and/or damages. However, the user of health and social care services can consent to the disclosure of information. In addition, disclosure may in certain circumstances be justified on the grounds that it is in the public interest (e.g. to help the police investigate a serious crime). Health and social care professionals should not, of course, obstruct police investigations, because that is itself a crime, but before making a disclosure they must satisfy themselves that it is sufficiently in the public interest to warrant waiving their duty of confidentiality. If they are not certain of this, confidentiality should be preserved and the reason for the decision should be explained to the police, who may then ask a judge to issue a witness summons on the basis that the public interest requires disclosure.

Human Rights Act 1998

The Human Rights Act 1998 incorporates the main Articles of the European Convention on Human Rights into the domestic law of all parts of the United Kingdom. The Human Rights Act obliges all public authorities to protect people's Convention rights and requires all other legislation to be applied, if possible, in a way which protects those rights. Article 8(1) of the European Convention states that: 'Everyone has the right to respect for his private and family life, his home and his correspondence.' To date this provision has not been interpreted by judges in the United Kingdom as imposing a right to privacy, but it has certainly been used to strengthen the right to confidentiality. The Convention itself recognizes limits to the right conferred by Article 8(1). Thus Article 8(2) provides:

There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a

democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

This means that any decision concerning the disclosure of confidential information about a user of health or social care services without his or her consent requires an analysis of whether the decision to disclose is 'proportionate'. The extent of disclosure should be proportionate to the purpose being fulfilled by the disclosure and should extend only as far as is necessary to achieve that purpose.

Data Protection Act 1998

The Data Protection Act 1998 gives effect throughout the United Kingdom to an EC Directive of 1995. It requires compliance with eight Data Protection Principles which set out standards for processing and handling information. The term 'processing' includes the collection, use and disclosure of personal data. The Data Protection Act is a central plank in the statutory framework underpinning confidentiality in the health and social care sectors. The following points are drawn from guidance issued by the Information Commissioner's Office in 2002:

The first data protection principle states that 'personal data shall be processed fairly, lawfully and shall not be processed unless at least one of the conditions in Schedule 2 is met and in the case of sensitive personal data at least one of the conditions in Schedule 3 is also met'. That is, there are three cumulative requirements of this principle:

(a) *The requirement to satisfy a condition in Schedules 2 and 3.* In practice it is unlikely to be difficult to satisfy the conditions of Schedules 2 and 3. Fundamentally, Schedule 2 requires that processing (use) is necessary for the exercise of functions of a public nature in the public interest by any person. Schedule 3 requires that processing is with the consent of the data subject, or that 'the processing is necessary for medical purposes and is undertaken by a health professional (or a person owing a duty of confidentiality equivalent to that owed by a health professional)'. The term 'medical purposes' embraces preventive medicine, medical diagnosis, medical research, the provision of care and treatment, and the management of healthcare services.

(b) *The requirement to collect personal information fairly.* There is an obligation on data controllers to provide certain information to data subjects when collecting their personal data. This is often referred to as 'fair processing information'. We should ensure that our patients are provided with the relevant details indicating the purposes for which their clinical

information is typically used. Details are required as to what information is being used.

(c) *The requirement to process personal information lawfully.* Fundamentally, the duty of confidence is under common law rather than statute.

The Data Protection (Processing of Sensitive Personal Data) Order 2000

Paragraph 10 of Schedule 3 to the Data Protection Act 1998 states that the processing of sensitive personal data can be carried out in circumstances specified by the Secretary of State. The Schedule to the *Data Protection (Processing of Sensitive Personal Data) Order 2000* specifies 10 such circumstances some of which could be relevant to information held by health and social care, particularly paragraph 4 (confidential counselling and advice and paragraph 5 (maybe in relation to health details of relatives used to calculate the life expectancy of an insured person)).

Freedom of Information Act 2000

The right under the Freedom of Information Act to request official information held by public bodies (known as the 'right to know') came into force in January 2005. Section 40 of the Act sets out an exemption from the right to know where the information requested consists of personal data. If the personal data is about the person requesting the information, then there is no right to know under the Freedom of Information Act. Instead, such requests are treated as 'subject access requests' under the Data Protection Act. If the personal data is about someone other than the applicant, there is an exemption from disclosure if disclosure would breach any of the Data Protection Principles.

The term "personal data" is defined as information about a living individual from which that individual can be identified. It may take any of the following forms:

- computer input documents
- information processed by computer or other equipment (e.g. CCTV)
- information in medical, social work, local authority housing or school pupil records
- information in some sorts of structured manual records
- unstructured personal information held in manual form by a public authority.

SPECIFIC LAWS

Criminal Law Act (NI) 1967

Section 5 of this Act imposes a duty on every person who knows or believes that an arrestable offence has been committed – and that he or she has information which is likely to secure the apprehension of someone for that

offence – to give that information, within a reasonable time, to the police. An arrestable offence is defined as one for which a person can be sent to prison for five years or more (i.e. a fairly serious offence). However a person can be charged with an offence under section 5 only if the Attorney General consents to this. Moreover a person who has been charged with the offence can plead by way of defence that he or she had a ‘reasonable excuse’ for not providing the information to the police. It is *possible* that a court would accept the public interest in preserving the confidentiality of service user information as a reasonable excuse for a professional in the health or social care sectors not passing on information about a crime to the police.

Public Health Act (NI) 1967

Under section 2 of this Act every medical practitioner attending on a person must, as soon as he or she becomes aware, or has reasonable grounds for suspecting, that that person is suffering from a notifiable disease, send to the Director of Public Health of the Health and Social Services Board for the area in which the examination took place a certificate stating (a) the name, age, sex and address of the patient, (b) the address of the building in which the examination took place, and (c) the notifiable disease from which, in the opinion of the medical practitioner, the patient is, or may be, suffering.

National Health Service (Venereal Diseases) Regulations 1974

These Regulations impose a duty on health authorities in Northern Ireland to ensure that information about venereal diseases obtained by their officers is treated as confidential. In 1991, Directions were made imposing the same obligations on trustees and employees of an NHS Trust.

Health and Safety at Work (NI) Order 1978

Articles 29, 29A and 30 of this Order regulate the duty to provide information in connection with the maintenance of health and safety in places of work. Generally speaking, no relevant information can be disclosed without the consent of the person by whom it was furnished, but there are exceptions for disclosure to, for example, a government department, an enforcing authority or the police.

Mental Health (NI) Order 1986

A psychiatrist who is arranging admission to a hospital under this Order is required to share relevant information with the approved social worker. The approved social worker must then consult with the nearest relative. Where the nearest relative requests discharge from hospital and the responsible medical officer issues a barring order, the responsible Board of the hospital is required to inform the nearest relative that the patient would be liable to act in a manner dangerous to others or to him- or herself. Mental Health Review

Tribunals and members of the Mental Health Commission can also access patients' records.

AIDS (Control) (NI) Order 1987

This Order imposes a duty on each health board in Northern Ireland to issue regular reports on the number, but not the names, of people diagnosed with AIDS and those who are HIV positive.

Human Fertilisation and Embryology Act 1990 This Act requires the Human Fertilisation and Embryology Authority, in particular circumstances, to disclose certain information it has recorded on a register it must keep. Some restrictions on the Authority's right to disclose were removed by the Human Fertilisation and Embryology (Disclosure of Information) Act 1992.

Police and Criminal Evidence (NI) Order 1989

Article 10 empowers the police to enter premises under a warrant issued by a magistrate to conduct a lawful search. The police can seize items if they are covered by the warrant or if there are reasonable grounds for believing that the items are evidence of an offence, but only if seizure is necessary to prevent the items being concealed or tampered with. Medical records, however, are within the definition of 'excluded material'. Generally speaking the police can gain access to and seize excluded material only after being granted permission by a judge. Where the police cannot rely on these statutory powers they may still make requests for disclosure of confidential documentation. In such instances health and social care professionals must decide whether it is in the public interest to disclose the confidential information to the police.

Criminal Appeal Act 1995

Section 17 states that where the Criminal Cases Review Commission (whose function is to identify miscarriages of justice) believes that a person serving in a public body has possession or control of a document or other material that may assist the Commission, the Commission may direct that person to produce the document or material to the Commission or to allow access to it. The Commission also has the power to order that the document or material must not be destroyed or altered. The duty to comply with the Commission's direction is not affected by any obligation of secrecy or other limitation on disclosure which would otherwise prevent the disclosure of the document or material.

Terrorism Act 2000

Under section 19 a professional person or employer commits a criminal offence if he or she does not disclose to the police – as soon as is reasonably

practicable – his or her belief or suspicion, and the information on which it is based, that another person has committed an offence relating to the funding of terrorism or to the use of property for the purposes of terrorism. However it is a defence for a person charged under section 19 to prove that he or she had a reasonable excuse for not making the disclosure. The Anti-terrorism, Crime and Security Act 2001 extends the disclosure requirements so that they apply even to terrorist investigations and proceedings being conducted outside the United Kingdom.

Sexual Offences Act 2003

Under sections 94 and 95 of this Act information given to the police about sex offenders can be supplied to a Northern Ireland Department for verification.

Serious Crime Act 2007

This Act amends the Audit and Accountability (NI) Order 2003 to give power to the Comptroller and Auditor General for Northern Ireland to conduct data matching exercises in order to assist in the prevention and detection of fraud. Data about patients can be used in data matching exercises only if the Comptroller requires it to be supplied by a body – such as a health board – whose accounts have to be audited by the Comptroller. In such cases the processing of data does not require the consent of the individuals concerned, but it must otherwise comply with the Data Protection Principles set out in the Data Protection Act 1998.

Appendix 3

PRIVACY ADVISORY COMMITTEE NORTHERN IRELAND

Chairman

Roy McClelland

*Emeritus Professor of Mental Health, Queen's University, Belfast
Consultant Psychiatrist, Belfast Trust*

Brice Dickson

Professor of Law, Queen's University Belfast

Mark Eustace EHSSB

*Information Systems Development Manager, Eastern Health and
Social Services Board*

Dr Grace Irwin

Assistant Director Informatics, Northern Health & Social Care Trust

Dr John Jenkins

*Senior Lecturer in Child Health, Queen's University Belfast,
Consultant Paediatrician, Antrim Hospital*

Ms Jan Maconachie

*Assistant Director Social Work/Care Education, Training and
Development, Northern Health & Social Care Trust*

Ms Maggie Reilly

Chief Officer Western Health and Social Services Council

DHSS Representatives

Mr David Reilly, Head of Information Branch
Mr Michael McArdle, Departmental Information
Manager

Project Manager

Mrs Eveline Fleeton, South Eastern HSCT

Appendix 4

Further Information and Guidance

Guidance on Privacy/Confidentiality Obligations for Health and Social Care Sector

Nursing and Midwifery Council (NMC), *Code of Professional Conduct: Standards for conduct, Performance and Ethics* (2008).

General Medical Council, *Confidentiality: Protecting and Providing Information* (April 2004).

<http://www.gmc-uk.org/guidance/current/library/confidentiality.asp>

General Medical Council, *Confidentiality: Frequently Asked Questions* (2004)

http://www.gmc-uk.org/guidance/current/library/confidentiality_faq.asp

General Social Care Council *Code of Practice for Social Care Workers* (September 2002)

<http://www.gsccl.org.uk/Good+practice+and+conduct/Get+copies+of+our+codes/>

Health Professions Council *Standards of Conduct, Performance and Ethics* (April 2003).

http://www.hpcuk.org/assets/documents/1000062CHPC034HPCA5_Standards_of_conduct_performance_and_ethics.pdf

British Medical Association, *Confidentiality and disclosure of health information* (1999)

Guidance on Consent and Capacity

Department of Health, Social Services and Public Safety, *Reference Guide to Consent for Examination, Treatment or Care* (March, 2003).

The Law Society/BMA *Assessment of Mental Capacity*, (BMA, 1995).

BMA, *Guidance on Consent and Capacity*.

<http://www.bma.org.uk/ap.nsf/Content/Hubethicsconsentandcapacity>

Guidance on Confidentiality and Children

Department of Health, Social Services and Public Safety, *Seeking Consent: Working with Children*

Department of Health, Social Services and Public Safety, *Consent—what you have a right to expect: a guide for parents.*

Department of Health, Social Services and Public Safety, *Consent—what you have a right to expect: a guide for children and young people.*

Department of Health, Social Services and Public Safety, *Co-operating to Safeguard Children*, especially Ch. 8 on 'Record Keeping, Confidentiality and Sharing Information'.

General Medical Council, *0-18 years: guidance for all doctors* (2007).

Royal College of Paediatrics and Child Health, *Responsibilities of Doctors in Child Protection Cases with regard to Confidentiality* (February 2004).

BMA, *Consent, Rights and Choices in Healthcare for Children and Young People*, (December 2000).

BMA, *Doctor's Responsibilities in Child Protection Cases* (June 2004).

Guidance on Handling Requests for Access to Personal Information

Department of Health, *Guidance for Access to Health records Requests under the Data Protection Act 1998.*

http://www.dh.gov.uk/Managingyourorganisation/Informationpolicy/Patientconfidentialityandcaldicottguardians/DH_4084411

Department of Health, *Frequently asked questions about accessing health records.*

http://www.dh.gov.uk/en/Managingyourorganisation/Informationpolicy/Patientconfidentialityandcaldicottguardians/FAQ/DH_065886

Extensive guidance on the operation of the Freedom of Information Act 2000 is available on the website of the Information Commissioner. In particular, see the guidance the exemptions for personal information and information provided in confidence. Also see the *Data Protection Technical Guidance Note No. 4: Dealing with subject access requests involving other people's information*.

<http://www.ico.gov.uk/>

British Medical Association, *Access to health records by patients Guidance for doctors on access to health records under the Data Protection Act 1998, and on access to the health records of deceased patients under the Access to Health Records Act 1990, or the Access to Health Records (Northern Ireland) Order 1993* (2002)

[http://www.bma.org.uk/ap.nsf/AttachmentsByTitle/PDFaccesshealthrecords/\\$FILE/Accessguidelines.pdf](http://www.bma.org.uk/ap.nsf/AttachmentsByTitle/PDFaccesshealthrecords/$FILE/Accessguidelines.pdf)

Department for Constitutional Affairs, *Handling Subject Access Requests under Section 7 of the Data Protection Act 1998* (April 2002)

<http://www.dca.gov.uk/foi/dpasaguide.htm>

Guidance on Data Protection

Information Commissioner, *The Data Protection Act 1998—Legal Guidance*,

http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/data_protection_act_legal_guidance.pdf

Information Commissioner, *Use and Disclosure of Health Data*, (May 2002)

http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/health_data_-_use_and_disclosure.pdf

Department of Health, *Data Protection Act 1998: Guidance to Social Services* (March, 2000)

Guidance on Human Rights Act 1998

OFMDFM, *Get in on the Act: Learning about the Human Rights Act*.

http://www.ofmdfmni.gov.uk/human_rights_reportnew1-3.pdf

Department for Constitutional Affairs, *Making Sense of Human Rights: A Short Introduction* (2006)

<http://www.dca.gov.uk/peoples-rights/human-rights/pdf/hr-handbook-introduction.pdf>

Department for Constitutional Affairs, *A Guide to the Human Rights Act 1998* (2006).

<http://www.dca.gov.uk/peoples-rights/human-rights/publications.htm>

Department for Constitutional Affairs, *Human rights: human lives - a handbook for public authorities* (2006)

<http://www.dca.gov.uk/peoples-rights/human-rights/pdf/hr-handbook-public-authorities.pdf>

Jeremy Croft, *Health and Human Rights: A Guide to the Human Rights Act 1998* (The Nuffield Trust 2003)

<http://www.nuffieldtrust.org.uk/publications/detail.asp?id=0&prID=18>

Department of Health/British Institute of Human Rights, *Human rights in Healthcare—A Framework for Local Action*, (2007)

http://www.bihhr.org/downloads/Health_framework.pdf

Other Relevant Guidance

BMA, *Guidance on Secondary Uses of Patient Information* (June, 2007)

BMA, *Guidance on Confidentiality and Disclosure of Information to PCTs in Primary Care Settings* (August 2007)

'*Good Management, Good Records*' – *Guidelines for Managing Records in Health & Personal Social Services Organisations in Northern Ireland*, (DHSSPS, December 2004)

HPSS ICT Security Policy, Directorate of Information Systems, Version 1.1 (DHSSPS, August 2003)

Department of Constitutional Affairs, *Public Sector Data Sharing: Guidance on the Law* (November 2003).

<http://www.dca.gov.uk/foi/sharing/toolkit/lawguide.htm>

Produced by: Department of Health, Social Services and Public Safety
Castle Buildings
Belfast BT4 3SQ
Telephone: 028 9052 2387
Textphone: 028 9052 7668
www.dhsspsni.gov.uk

January 2009