



Health and Social Care

Draft Code of Practice on Protecting the Confidentiality of
Service User Information

Version 7.1

11 May 2007

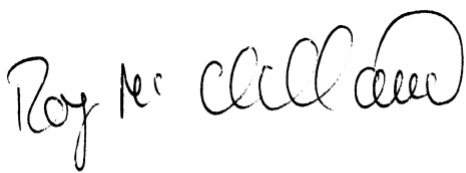
DRAFT

Foreword

The Privacy Advisory Committee (Northern Ireland) was established in 2006 to oversee the implementation of recommendations agreed by Minister on Protecting Personal Information. The recommendations included the development of a comprehensive Code of Practice on Confidentiality to replace existing guidance.

The aim of the Code of Practice is to support all staff in making good decisions about the protection, use and disclosure of service user information. Careful consideration has been given to the wide range of situations and purposes in which the use or disclosure of service user identifiable information may be considered.

The Committee gratefully acknowledges the helpful comments received on earlier drafts from the General Medical Council, the Information Commissioner's Office and the Confidentiality Unit of the Department of Health in Leeds.



Roy McClelland

Roy McClelland
Chairman, Privacy Advisory Committee (Northern Ireland)

Contents

1. Introduction	1.1 – 1.6
2. Protection of service user information	2.1 – 2.22
Ethical obligations to protect service user privacy	2.4 – 2.8
Legal obligations to protect service user privacy	2.9 – 2.12
The general requirement to keep service users informed	2.13 – 2.22
3. Consent for the use or disclosure of service user information	3.1 – 3.20
Disclosure after a service user’s death	3.3 – 3.4
Consent in the provision of direct care to the service user	3.5 -3.14
Lack of capacity	3.9 – 3.13
Emergency situations	3.14
Consent for use and disclosure of information for purposes of health and social care not directly related to care of that service user	3.15 – 3.18
Consent and the use and disclosure of information for purposes not related to the care of the service user	3.19 – 3.20
4. Information Handling	4.1 – 4.13
The service user’s general right of access to their health and social care records	4.4
Respect for privacy in seeking service user information	4.5 – 4.7
Maintaining information in a form which protects the identity of the service user	4.8 – 4.12
Managing information and records	4.13

5.	The purpose of any anticipated use or disclosure of service user information	5.1 – 5.28
	Use and disclosure of information for the direct care of that service user	5.5 – 5.13
	Review of care, including audit	5.6
	Multidisciplinary teams and inter-agency Working	5.7 – 5.9
	Sharing information and informal carers	5.10 – 5.11
	Dual roles	5.12 – 5.13
	Use and disclosure of information for purposes of health and social care not directly related to care of that service user (secondary uses)	5.14 – 5.19
	Use and disclosure of information for purposes not related to the care of the service user	5.20 – 5.28

Appendix 1:	Simplified good practice model
Appendix 2:	Examples of confidentiality decisions in practice
Appendix 3:	Examples of confidentiality obligations from professional codes of ethics
Appendix 4:	Common law of confidentiality
Appendix 5:	European Convention on Human Rights and Human Rights Act 1998
Appendix 6:	Data Protection Act 1998
Appendix 7:	Good practice in making discretionary disclosures in the public interest
Appendix 8:	Handling requests for access to personal information
Appendix 9:	Good practice in making decisions about information use or disclosure with service users lacking capacity
Appendix 10:	Examples of statutes prohibiting, requiring or permitting disclosure of confidential information
Appendix 11:	International Standards

Further Information and Guidance

Chapter 1. Introduction

- 1.1 People who use health and social services have a range of rights and those who provide health and social care and services have a range of obligations to service users. Key obligations of all staff are to respect the privacy and confidentiality of service users.
- 1.2 All health and social care staff have strong *ethical* obligations to protect the information of service users which are recognised in professional ethical codes. There are also *legal* obligations to protect service user information. The legal and ethical obligations of all health and social care staff to protect the privacy of service users form a key part of their general obligation to protect service users from harm. It forms part of the general obligation to provide a service which is respectful of and actively promotes the human rights and dignity of service users.
- 1.3 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 a discussion of the principles which underpin both the ethical and various legal frameworks. It provides a method for considering decisions concerning service user information in the light of these key frameworks thus avoiding unnecessary legal technicality.
- 1.4 This Code of Practice provides:
 - information on the ethical and legal obligations of health and social care staff;
 - consideration of the principles which underlie both the ethical and various legal obligations;
 - practical guidance to assist decision-making with respect to service user information;
 - a method for considering decisions concerning service user information.
- 1.5 The Code of Practice on Confidentiality 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.

- 1.6 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. This Code of Practice cannot be taken as an authoritative statement of the law and legal advice should be sought when necessary.

DRAFT

Chapter 2. Protection of service user information

- 2.1 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.
- 2.2 It is important to note that legal consequences may follow from a breach of ethical standards set by regulatory authorities.
- 2.3 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

- 2.4 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 privacy and confidentiality 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.
- 2.5 The relationship between health and social care staff and the service user should be one of 'fidelity' or 'trust'. Within the relationship between a member of health and social staff and the service user, there exists a tacit understanding on the part of the service user that private information will not be further used or disclosed without the awareness and consent of the service user.
- 2.6 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 how it may be used.
- 2.7 One reason for respecting confidences in health and social care is that doing so enables service users to disclose the 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, for public health and for health and social care practice.

2.8 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 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 greater when the combined weight of 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

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

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

2.10 The nature and level of protection offered by each 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.

2.11 Further information about these laws and references to relevant further guidance is provided in Appendices 4, 5 and 6.

2.12 In some circumstances it will be appropriate to consult with a legal representative of the service user. By this is meant someone provided for by law to represent the interests of, and/or take decisions on behalf of, a person who does not have the capacity to consent. This would include the parent or guardian of a minor. It may also 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. Further guidance about good practice in making decisions with service users lacking capacity can be found in Appendix 9.

The general requirement to keep service users informed

- 2.13 Service users must be kept informed about the possible uses and disclosures of their information so that they are in a position to exercise their legal rights and enjoy the full protection of the relevant laws. It is also necessary to ensure that any consent they give is sufficiently informed to be valid and to ensure that the data controller meets its fair processing obligations under the Data Protection Act 1998.
- 2.14 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 (see Appendix 10) and of the duty of health and social care staff to protect important public interests (see 5.18–5.25 and Appendix 7).
- 2.15 Modern health and social care services often involve sharing information between staff to provide optimal care and treatment. Service users must be made aware of what information is held about them, the purposes for which the information is used and the people with whom such information may need to be shared to provide their care. They must also be informed that it may be used to support clinical audits and other work to monitor the quality of care provided. Service users also need to be aware of the choices they have for particular uses and disclosures of the information.
- 2.16 It is an ethical and legal requirement that patients are kept informed of all circumstances in which they can give, withhold or withdraw consent to the use of their information. They must also be given the information necessary for that consent to be valid.
- 2.17 It is not necessary to inform service users in exhaustive detail of all uses and disclosures and potential uses and disclosures of their information. It is important to note that service users cannot give valid consent to what they are unaware of and information provided to them must be sufficient for this purpose. It may be necessary to provide additional information in particular situations; for example when their information is being passed to a registry.
- 2.18 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.
- 2.19 Service users should be informed of the categories of people and organisations to which information may need to be passed for health and social care services to function. 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 any aspects. It should be made clear to service users that they may object to specific secondary uses of identifiable service user information and that their objection will be respected.
- 2.20 In circumstances where a legal obligation or justification for use or disclosure without consent exists (see 5.18-5.19), service users should still usually be informed about the use of their information. Service users must in general be informed of all uses or disclosures, even when they have no choice over whether or not they occur. It is important that this information is provided in a manner appropriate for the service user's communication needs.
- 2.21 It may not always be appropriate to provide information to a service user about particular uses and disclosures of their information. For example, where a service user lacks capacity, information provision should take place with full consideration being given to their best interests.
- 2.22 Three key reference points which should usually be considered when addressing a particular question concerning service user privacy are 'consent', 'information' and 'purpose'.
- *Consent.* As with any other intervention in health or social care, one of the most important and effective protections for service users is the requirement to gain their consent before any use or disclosure of their information. (See Ch. 3)
 - *Information.* The nature and content of the information in question determines to some extent which particular laws apply and whether a particular use or disclosure is ethically and legally permissible. (See Ch. 4)
 - *Purpose.* The intended purpose is of central importance in determining which protections govern disclosure and how they apply. It is only when one is clear about the purpose of an intended use or disclosure that one can be certain whether it is ethically or legally permissible. (See Ch. 5)

Appendix 1 provides decision trees to assist in reaching an overview of the particular issues arising in connection with each element. Examples of how good decisions are made in practice with due consideration of these elements are provided in Appendix 2.

DRAFT

Chapter 3. Consent for the use or disclosure of service user information

- 3.1 Consent is a means by which the competent service user can exercise control over the dissemination of their confidential information. The justification for use or disclosure of person identifiable information should normally be the consent of the service user. As well as generally being an ethical and/or legal requirement, gaining the consent of the service user empowers them, protects their dignity and builds trust with staff. Consent requirements may differ depending upon the purpose of the intended use or disclosure (see 5.1–5.3).
- 3.2 If the service user who has capacity refuses to consent to disclosure, the information cannot be disclosed, unless, exceptionally, a justification other than consent exists. Health and social care staff should discuss with the service user why he/she thinks that disclosure is in the service user's best interests. It is never justified to disclose information in the 'best interests' of the service user with capacity who refuses to consent to disclosure.

Disclosure after a service user's death

- 3.3 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
- 3.4 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.

Consent in the provision of direct care for the service user (see 5.5)

- 3.5 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 of what information sharing is necessary for their care. Provided they are informed in this way (see 2.13-2.21), express consent is not necessary. The consent of the service user to the disclosure of information necessary for their care may be inferred from their acceptance of that care.
- 3.6 The compliance of a service user alone is not sufficient basis 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. If there is doubt that these conditions are fulfilled, then an expression of consent should be sought from the service user.

- 3.7 In practice, staff should ask themselves if an onlooker would reasonably conclude that the service user had agreed to the disclosure taking place. If there is doubt that they would, then valid consent has probably not been obtained. Where there is doubt, staff should in seek an expression of consent to confirm the actual consent from the service user for that disclosure.
- 3.8 There are circumstances where a service user is unable or no longer able to consent to the use or disclosure of their confidential information (such as when the service user temporarily lacks capacity or in an emergency) and in such circumstances special considerations apply.

Lack of capacity

- 3.9 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. The protection of the privacy interests of service users who lack capacity is in general in their best interests. In particular situations, their privacy interests must be balanced against their other interests (such as their health and social care) to ensure an outcome which is in their overall best interests. As with other service users, there remains a possibility of a public interest which overrides the public interest in maintaining the confidentiality of service users who lack capacity.
- 3.10 Where a service user lacks capacity disclosure can be justified to protect their best interests. Whether disclosure is justified on this basis in the particular situation depends on a weighing of the service user's interest in having the confidentiality of his/her information maintained and the interests that are at risk without disclosure. (See Appendix 9 for further guidance on good practice decision-making with service users who lack capacity.)
- 3.11 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 unnecessarily disclosing confidential information to them. Such a disclosure may not itself be in the best interests of the service user.
- 3.12 The normal principles on disclosing confidential information in the public interest (see 5.18-5.25) or in accordance with statute (see Appendix 10) also apply to the confidential information of service users lacking decision making capacity with respect to uses and disclosures of their information.

- 3.13 Where a member of health and social care staff thinks that disclosure would be in the best interests of a service user who lacks the capacity to give or withhold consent, he/she should in general raise this with a legal representative (see 2.12) of the service user. If the consent of such a legal representative is withheld, the member of health and social care staff might involve the court to settle the dispute.

Emergency Situations

- 3.14 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. Due care should be exercised not to override any relevant legally binding wishes of the service user which have been expressed in advance of the situation arising.

Consent for use and disclosure of information for purposes of health and social care not directly related to care of that service user (see 5.14)

- 3.15 While the behaviour of a service user can provide a basis for inferring their consent to the use and disclosure of information for their care, there is no behaviour which clearly indicates consent to other uses.
- 3.16 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. 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 unless a statutory basis for the use or disclosure exists or there is an overriding public interest in the use or disclosure. In the absence of one of these legal bases, the norm should be that service user information will not be used without their express consent.
- 3.17 When consent is refused, service user information should in general not be used.
- 3.18 Situations arise where the consent of service users cannot readily be obtained for use or disclosure yet there are clearly important public health and social care interests in such uses, e.g. cancer registries. In England and Wales legislation has been introduced to allow confidential information to be disclosed and used for health purposes where it is not practicable to satisfy the common law requirement of obtaining consent. The Privacy Advisory Committee has requested that the DHSSPS consider the need for appropriate provision to allow specific secondary health and social care uses in Northern

Ireland with appropriate safeguards and restrictions. Further guidance on use and disclosure for secondary purposes is given below (see 5.14-5.17).

Consent and the use and disclosure of information for purposes not related to the care of the service user (See 5.18)

- 3.19 There are situations in which it may be ethically and legally permissible for health and social care staff to disclose confidential information for a purpose not related to the care of that service user—for example, prevention of harm to a third party (see 5.18-5.26). 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 be appropriate to seek consent in order to protect the relationship with the service user. Consent should not be sought where there is an overriding public interest and where doing so would prevent achieving the justified aim of the disclosure or where doing so would put the safety of the member of staff at risk.
- 3.20 Exceptions to this normal procedure are 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 at risk.

4. Information Handling

- 4.1 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. The protection of the privacy of the service user requires attention to the manner in which the confidential information in the record is obtained, to how it is held and to how it is disposed of.
- 4.2 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. If a refusal to consent to professional record keeping has implications for their care, this must be discussed with the service user.
- 4.3 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 not only to process more personal information (for example, in new contexts, or through aggregation) but also to make a service user's information more readily available to a wider range of people than a hard copy record. The use of electronic records tends to transgress the traditional boundaries of the individual service user's direct relationship with a professional. The relative ease of access to health and social care information stored in an electronic record might also attract additional attention from third parties such as law enforcement agencies. For these reasons, the benefits of implementing electronic systems for holding records must be reviewed in the light of existing legal and ethical obligations and for the need for additional safeguards.

The service user's general right of access to their health and social care records

- 4.4 Service users have a general right to access their health and social care records. There are two possible reasons for not disclosing the requested information. Information in the record about third parties should not in general be disclosed without their consent. 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.

Respect for privacy in seeking and in using service user information

- 4.5 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.

- 4.6 Private information should only be requested from 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 the service user. Any means of communication of private information (for example, telephone or email) should also be sufficiently secure to ensure the privacy of the service user.
- 4.7 If a member of staff is seeking information from another member of staff, then it should only be sought from someone with the authority to disclose that information. Ethical and legal information flows require that those disclosing information have the necessary authority to do so. 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.
- 4.8 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.
- 4.9 Service user information should not be moved to a less secure environment unless this cannot be avoided. Particular care is needed when traveling and portable computers, notes and files must not be left unattended or in easily accessible areas.

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

- 4.10 Service user information should be kept in a form and in a manner which protects the identity and privacy of the service user. The highest standards of security should apply to service user information and staff should reasonably satisfy themselves that information they disclose will be kept in a manner which is in keeping with such standards.
- 4.11 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).

- 4.12 '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.
- 4.13 Anonymisation and pseudonymisation are key means for protecting the rights of service users. Where appropriate, the DHSSPS should aim to anonymise or pseudonymise information. 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.
- 4.14 Many secondary uses of service user information do not need to identify service users and in such situations the information should be held in the form which most protects the identity of the service user. The exception to this is where identification is strictly necessary for the secondary purpose. (Also see 5.14-5.17.)

Managing Information and Records

- 4.15 Good records management standards and practices underpin respect for the privacy of service user's information. Specifically, it is vital 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 an organisations' disposal schedule. Similarly, access to electronic records should be appropriately protected.

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

5.1 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.

5.2 It is a general ethical and legal principle that to be proportionate any use or disclosure must only be of the minimum amount of information necessary to achieve the purpose of that disclosure or use. It is only when the purpose of any intended use or disclosure is clear that the minimum necessary information to achieve that purpose is also clear.

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

- (A) use and disclosure of information for the direct care of that service user;
- (B) use and disclosure of information for purposes of health and social care not directly related to the care of that service user (secondary uses);
- (C) use and disclosure of information for purposes not related to the care of the service user.

Any acceptable use or disclosure will necessarily fall under one of these three general types of purpose. Best practice in the ethical and legal decision-making process differs depending upon the purpose of the contemplated use or disclosure.

5.4 A simplified good practice model of the decision-making process which uses these distinctions is provided in Appendix 1. It draws attention to the most relevant considerations for each purpose.

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

5.5 If the use or disclosure is necessary to provide the care for that service user, then their consent to the use or disclosure can be inferred from their acceptance of the care. The test is not whether a use or disclosure would benefit the service user, but rather if the use or disclosure is for the purpose of the direct care of the service user.

Review of care, including clinical audit

5.6 Health and social care governance, including audit, carried out by members of the care team of their own performance in caring for the service user is for the

purpose of improving the direct care of that service user. It has sufficient connection with that direct care to be justified on the basis of inferred consent.

Multidisciplinary teams and inter-agency working

- 5.7 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.
- 5.8 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.
- 5.9 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. The purpose of involving the other agency should be clarified along with the purpose of the proposed information sharing. Where a service user refuses to consent to the involvement of other agencies their refusal should be respected unless there are overriding interests (see paragraphs 5.18-5.25). Where other agencies request information about service users, health and social care staff should first seek the consent of the service user or their legal representative about such sharing.

Sharing information and informal carers

- 5.10 Family members and other persons who are providing important 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 and with any legal representative (see 2.12).
- 5.11 Reasonable steps should be taken to protect the privacy and confidentiality of informal carers. A carer may share information for the benefit of improved care

for the service user on the understanding that it may not be disclosed to the service user that such information sharing has taken place. The interests of carers must be protected and in general their right to privacy and confidentiality should be respected.

Dual roles

- 5.12 Health and social care staff may work in situations where they may have dual roles with dual and conflicting responsibilities and obligations. This includes work in prisons and for court liaison schemes where there are duties to both the service user and to the authority. Such dual roles and obligations may cause conflict about the confidentiality of service user information. For example, a prisoner or defendant may have consulted a healthcare professional and divulged information that they do not wish an outside agency to know, while in their current role the healthcare professional may be obligated to disclose that information.
- 5.13 Health and social care staff should avoid situations with dual responsibilities and obligations to the same service user wherever possible. 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 when the information given will not be treated as confidential. It is important to note that staff cannot 'contract' out of their professional obligations with respect to service user confidentiality.

(B) Use and disclosure of information for purposes of health and social care not directly related to care of that service user (secondary uses)

- 5.14 Some uses and disclosures of service user information are for purposes of health and social care but do not aim at 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. 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.
- 5.15 Where there is a clearly overriding public interest in accessing service user information for broader health and social care purposes, there will usually be a legal *obligation* to disclose the information. However, other secondary uses may be strongly in the public interest and have a legal *justification* even though they are not obligatory. The conditions which make such uses permissible are not the same as in cases of discretionary disclosures in cases where the public

interest overrides the obligation of confidentiality (see 5.24-5.28). In particular, service users retain the right to opt out of specific secondary uses of their personal identifiable information. Such secondary uses are only justified where the service user has not expressed dissent to such use.

- 5.16 In the case of a legally obligatory disclosure or a legally justified disclosure for purposes of health and social care not directly related to care of that service user, ethical standards must also be satisfied. This may in some cases include a need for formal approval by a research ethics committee.
- 5.17 Although the disclosure of confidential information can be justified in the public interest, such a justification is problematic for secondary purposes. Secondary uses tend to be made on the basis of a general policy, not on the basis of case by case assessment. The public interest justification for disclosure is available to health and social care staff in the particular circumstances of specific cases where a weighing of the private and public interest in maintaining confidentiality against a competing public interest can be performed. As secondary uses often involve administrative procedures being applied to all cases, no such balancing exercise is being performed and the required judgment of the proportionality of the disclosure in each case is not being made.
- 5.18 The Patient Information Advisory Group (PIAG) for England and Wales (established under Section 60 of the Health and Social Care Act 2001) has identified principles for good practice for situations where balancing is required between maintaining confidentiality or obtaining consent and a strong public interest in the running of an efficient and quality health service. Although PIAG is without legal authority in Northern Ireland, these principles form a useful guide to good practice.
- 5.19 The Privacy Advisory Committee endorses the following principles for good practice in situations where balancing is required between maintaining confidentiality or obtaining consent and a strong public interest.
- 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 quickly implement procedures for obtaining the express consent of the service user.
 - ‘Third Party’ organisations seeking information other than for direct care should be seeking anonymised or pseudonymised data. (See 4.18-4.12)

- Any use must be of clear general good or of benefit to service users.
- Provisions for non-consensual use of service user identifiable information should only be temporary, with a clear ‘exit strategy’ with defined end dates for one of the following solutions:
 - service user consent;
 - anonymisation; or
 - explicit legal support.
- Organisations should not hold 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.

(C) Use and disclosure of information for purposes not related to the care of that service user

- 5.20 It is sometimes both legally and ethically acceptable to use or disclosure service user information for purposes which are neither related to the care of that service user nor for a secondary health and social care purpose. Examples of such purposes include: prevention of harm to third parties; child protection; protecting vulnerable adults; prevention of terrorism; misuse of controlled drugs; investigation of serious professional misconduct.
- 5.21 Disclosures of this kind might be *legally obligatory*, that is, the law does not leave staff the discretion not to make them. They might be *legally justifiable*, that is, the law permits staff to make decisions about disclosure on a case by case basis, but it does not require them to do so.
- 5.22 In the case of a legally obligatory disclosure or a legally justified disclosure, ethical standards must also be satisfied. The considerations relevant to the legal assessment of a potentially justifiable disclosure are also relevant to its ethical assessment.
- 5.23 Where a statute imposes a strict requirement to disclose information, care should be taken only to disclose the information required to comply with and fulfil the purpose of the law. 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.

- 5.24 Discretionary disclosure of confidential information to parties outside health and social care services, in the absence of consent or presence of dissent, may be justifiable in order to protect an overriding public interest, including the public interest in the protection of individuals. The third parties to be protected may be outside health and social services or may be other service users or members of staff.
- 5.25 Disclosure will only be justified in exceptional circumstances, that is, if the disclosure serves an interest that in the particular circumstances outweighs the service user's right to privacy. Disclosures of this nature will be relatively rare and should take place on the basis of established formal procedures.
- 5.26 The purposes outside health and social care for which health and social care information are requested can change in changing social, economic and political climates. It is important that the interests of service users do not become subordinate to the general interest of society, but 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. (For further guidance on human rights law, see Appendix 5).
- 5.27 In all cases of discretionary disclosure in the public interest, there is no obligation to disclose, but whether or not disclosure can be justified rather depends on balancing the interests that are in conflict in each case. 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.
- 5.28 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 in the public interest. 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. (For further guidance for making good decisions in the public interest see Appendix 7.)

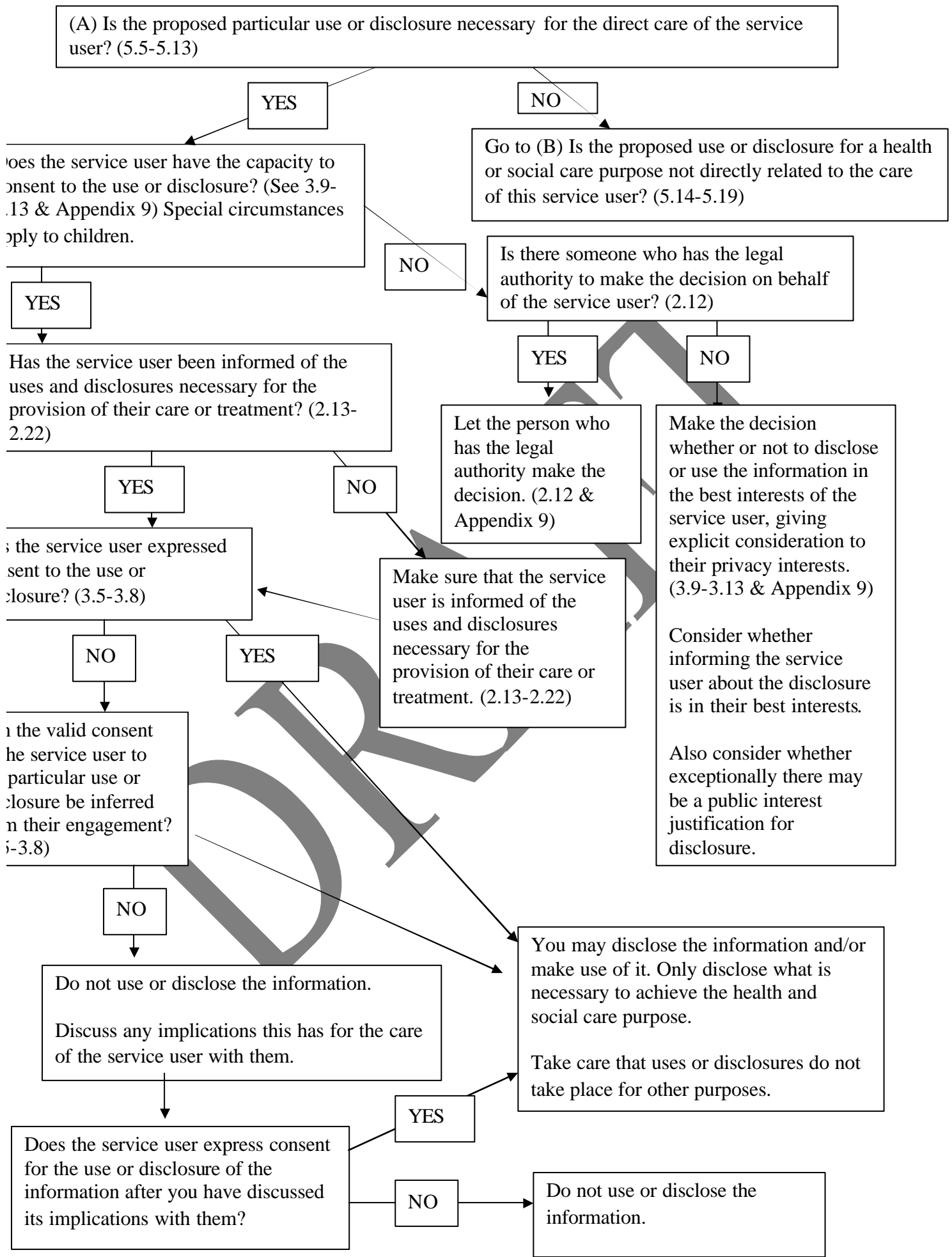
Appendix 1: Simplified Good Practice Model

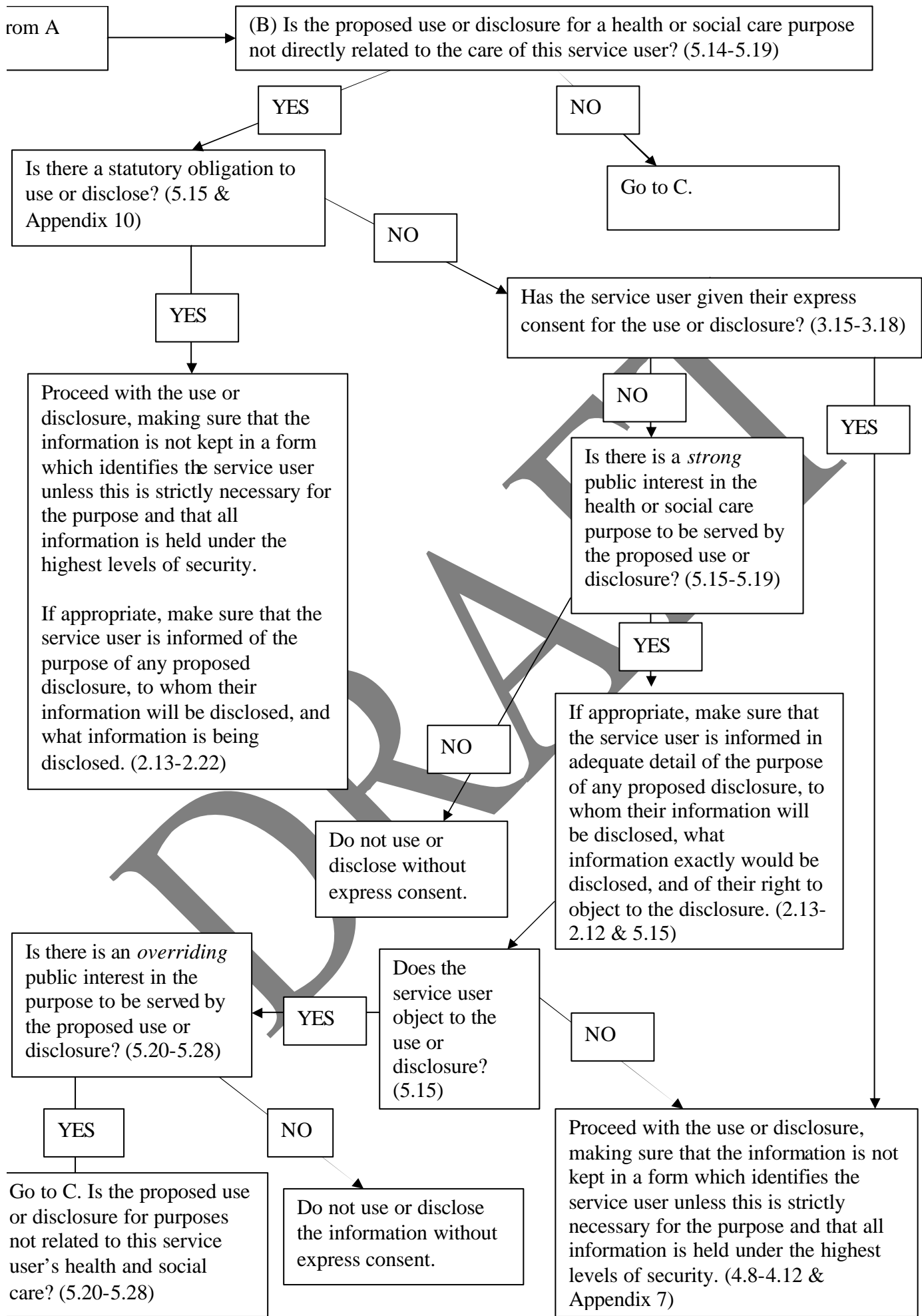
The following flow charts provide a simple tool to direct your attention to the key considerations in making good decisions about the use and disclosure of personal identifiable service user information. It must be used in conjunction with the body of this Code of Practice and it contains references to the particularly relevant paragraphs in brackets.

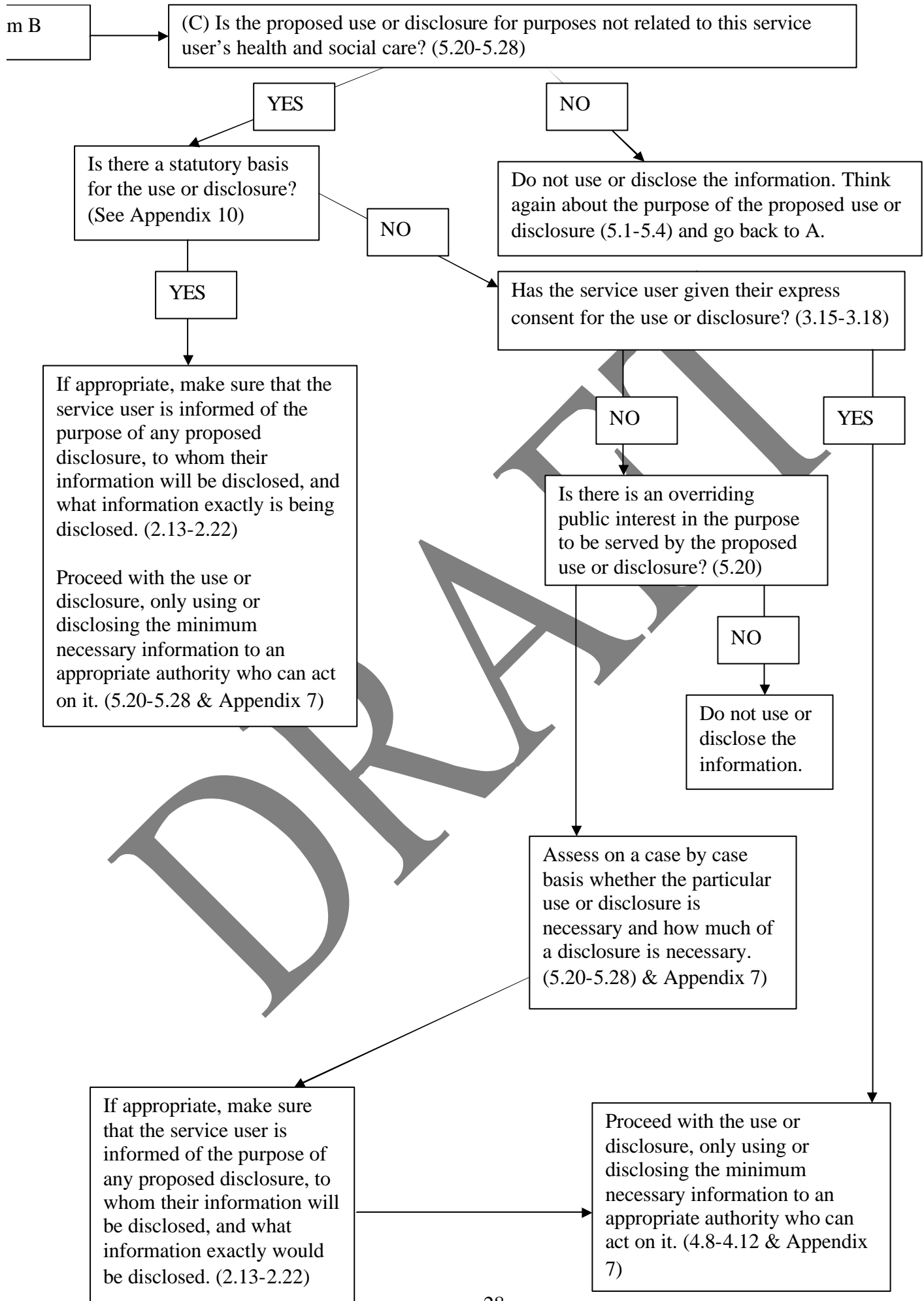
The chart falls into three sections which correspond to the distinction in the text between the three kinds of purpose of any proposed use or disclosure. These three purposes are:

- (A) use and disclosure of information for the direct care of that service user;
- (B) use and disclosure of information for purposes of health and social care not directly related to care of that service user;
- (C) use and disclosure of information for purposes not related to the care of the service user.

Any acceptable use or disclose will necessarily fall under one of these three general types of purpose, although this is not sufficient to guarantee its acceptability. Best practice in the ethical and legal decision-making process differs depending upon the purpose of the contemplated use or disclosure.







Appendix 2: Examples of Confidentiality Decisions in Practice

Scenario 1: Lack of capacity

Client has had a brain injury. His cognitive functioning is compromised and as a result he has problems making decisions for himself. He lives with his next of kin who provides a lot of support and care. Other family members have contacted the service requesting information on the client. The family members who have requested information do not communicate with the rest of the family and have not seen the client for a significant period of time but are keen to re-establish contact.

Discussion

The key question for Scenario 1 is that of the purpose of the contemplated disclosure. Whilst of potential benefit to the service user, disclosing information to the relatives now seeking contact is not necessary for the care of the service user and this is the only likely justification. It is not clear whether the service user has the capacity to make this decision for himself nor that it is in his best interests.

Scenario 2: Child Protection

16 year old girl is now living back at home, after being 'looked after' in a Residential Unit for a number of months as her behaviour was out of the control of her parents. Much of this behaviour was destructive, some self destructive, including self harming. She is making considerable progress with the help of a Social Worker specially trained in child psychotherapy. As part of the 'contract' with the Social Worker she has signed a document indicating that she understands that confidentiality may be limited for Child Protection reasons. She has disclosed (reluctantly) recently that her father was an aggressive man and frequently 'beat up' her mother, and occasionally beat herself and her siblings. This has been shared with the family with the objective of trying to support the father to undertake Anger management classes.

The work has now become 'stuck' due to the girl's unwillingness to disclose any further information about her difficulties, explaining that she would not be prepared to have anyone else know about 'her secrets'. The Social Worker suspects that the secrets relate to sexual abuse because of some of the girl's comments. The girl is beginning to behave more irresponsibly again, and when pressed indicates that she wants to move on, but because of the fact that her wishes for confidentiality will not be respected, she is not prepared to disclose anything further. She also quotes the 'Gillick' case as proof of protection of young peoples rights.

Discussion

The purpose of the disclosure that is being contemplated in Scenario 2 is not related to the health and social care of the service user, namely, the prevention of crime and the protection of children. There is no statutory basis for such disclosure, but rather it might be justified as being sufficiently in the public interest to outweigh the public

interest in the maintenance of confidentiality. This is because the girl has withheld consent to any disclosure to others. It looks likely that she has the capacity to withhold such consent and can do so even against her best interests. However, it is likely in such a case that the public interest would justify disclosing to the relevant authorities. The existence of the 'contract' may help maintain the relation with the social worker, but is unlikely alone to meet the ethical obligation on the part of the social worker to protect the confidentiality of the service user.

Scenario 3: Disclosing to other members of staff

A registered Paramedic is transferring a patient from one hospital to another. Should a Staff Nurse in the hospital inform the Paramedic of the patient's medical condition prior to transfer?

Discussion

When another health and social care professional is taking over the care of a service user, it is necessary to disclose the information that they need to provide the care appropriate to their role. Such disclosures are necessary for the care of the service user and can be made if the member of staff can infer the consent of the service user to such disclosures.

Scenario 4: Access to GP patient records by Drug Company Employees.

A drug company has an active programme of assisting GPs with patient management by reviewing their records (on a specific group of patients, diabetics) and then providing review clinics for those patients. A drug company is seeking to provide this service to a GP practice.

Discussion

This form of audit of the care of service users involves access to their records by people who are not actively involved in their care and as such service users must be informed about such potential disclosures and of their right to object. The express consent of service users is necessary to justify such disclosures. In addition to such consent on the part of the service users, binding confidentiality obligations must be established on any non-practice or HPSS personnel undertaking such audit and it must be established that appropriate security measures will be in place to protect service user information throughout the audit.

Appendix 3: Examples of Confidentiality Obligations from Professional Codes of Ethics

The general duty to maintain confidentiality and respect privacy is recognised by professional ethical codes which apply to health and social care staff.

Some examples are given below and it is important that staff consider all of the professional guidance that applies to them. The absence of professional status or of an explicit duty to maintain confidentiality in a code of professional ethics does not mean that the member of health and social care staff does not have an obligation to protect the confidentiality and privacy of service users. All staff are under such an ethical obligation.

The General Medical Council (GMC) Guidance on *Confidentiality: Protecting and Providing Information* (2004) states that:

Patients have a right to expect that information about them will be held in confidence by their doctors. Confidentiality is central to trust between doctors and patients. Without assurances about confidentiality, patients may be reluctant to give doctors the information they need in order to provide good care. If you are asked to provide information about patients you must:

- inform patients about the disclosure, or check that they have already received information about it;
- anonymise data where unidentifiable data will serve the purpose;
- be satisfied that patients know about disclosures necessary to provide their care, or for local clinical audit of that care, that they can object to these disclosures but have not done so;
- seek patients' express consent to disclosure of information, where identifiable data is needed for any purpose other than the provision of care or for clinical audit ...
- keep disclosures to the minimum necessary; and
- keep up to date with and observe the requirements of statute and common law, including data protection legislation.

The Nursing and Midwifery Council (NMC) *Code of Professional Conduct: Standards for Conduct, Performance and Ethics* states that:

5. As a registered nurse, midwife or specialist community public health nurse, you must protect confidential information
- 5.1 You must treat information about patients and clients as confidential and use it only for the purposes for which it was given. As it is impractical to obtain consent every time you need to share information with others, you should ensure

that patients and clients understand that some information may be made available to other members of the team involved in the delivery of care. You must guard against breaches of confidentiality by protecting information from improper disclosure at all times.

5.2 You should seek patients' and clients' wishes regarding the sharing of information with their family and others. When a patient or client is considered incapable of giving permission, you should consult relevant colleagues.

5.3 If you are required to disclose information outside the team that will have personal consequences for patients or clients, you must obtain their consent. If the patient or client withholds consent, or if consent cannot be obtained for whatever reason, disclosures may be made only where:

- they can be justified in the public interest (usually where disclosure is essential to protect the patient or client or someone else from the risk of significant harm);
- they are required by law or by order of a court.

5.4 Where there is an issue of child protection, you must act at all times in accordance with national and local policies.

The Health Professions Council *Standards of Conduct, Performance and Ethics* (2003) affirms similar standards for the protection of the confidentiality of service users as those set for doctors and nurses:

2. You must respect the confidentiality of your patients, clients and users.

You must treat information about patients, clients or users as confidential and use it only for the purpose for which it was given. You must not knowingly release any personal or confidential information to anyone who is not entitled to it, and you should check that people who ask for information are entitled to it.

You must only use information about a patient, client or user:

- to continue to care for that person; or
- for purposes where that person has given you specific permission to use the information.

You must also keep to the conditions of any relevant data-protection legislation and follow best practice for handling confidential information relating to individuals at all times. Best practice is likely to change over time, and you must stay up to date. You must be particularly careful not to reveal, deliberately or accidentally, confidential information that is stored on computers.

The *Code of Practice for Social Care Workers* of the Northern Ireland Social Care Council (NISCC) states that social care workers 'must protect the rights and promote the interests of service users and carers. This includes respecting and maintaining the dignity and privacy of service users'. It also states that social care workers 'must strive to establish and maintain the trust and confidence of service users and carers.

This includes respecting confidential information and clearly explaining agency policies about confidentiality to service users and carers’.

Further guidance which articulates similar obligations is also produced by professional associations and Royal Colleges. Ethical standards of professional codes of conduct are written in the light of the legal obligations on health and social care professionals. It is unlikely that someone would be breaching confidentiality in a legal sense if they were acting in keeping with the ethical standards of conduct defined by a professional regulatory authority. However, the reverse does not necessarily apply as ethical standards are often set higher than legal standards.

DRAFT

Appendix 4: Common law of confidentiality

The common law is the law that develops over time through the decisions of judges in particular cases. This legal sense of ‘confidential’ is narrower than the everyday use of term as a synonym for ‘private’ or ‘secret’. Nor is something legally confidential simply because it is marked as such.

A breach of confidentiality in the legal sense would traditionally only arise where the following three prerequisites exist:

- 1) where the information has the necessary quality of confidence, i.e. it is private and is not in the public domain
- 2) where the information was imparted in circumstances that create an obligation of confidence (for example, in the context of the relationship between a member of health and social care staff and service user relationship)
- 3) where unauthorised use of the information would have a detrimental effect on the patient.

If one or more of the above elements is missing there would be no breach of confidentiality.

For a justified disclosure of confidential information in the common law, the *actual consent* of the service user (which can be express or implied) is required unless there is an overriding public interest or a statutory basis permitting or requiring disclosure.

Recent case law has extended the applicability of the obligation of confidence to include situation where there is no pre-existing relationship between the parties in which the information was confided. The law on confidentiality is now broader in that it protects one against the misuse of one’s personal information. This development is clearly in keeping with the existing obligations on health and social care staff.

As well as having a legal meaning, ‘confidentiality’ is also an ethical obligation and all staff should consult all relevance ethical guidance for detailed information on their ethical obligations in this respect. (See Appendix 3 for examples from professional codes on the ethical obligation to maintain confidentiality.)

Appendix 5: European Convention on Human Rights and the Human Rights Act 1998

The Council of Europe's *Convention for the Protection of Human Rights and Fundamental Freedoms* (ECHR) (ETS n° 005, 1950 as amended) is an international treaty which is binding on all those states that have ratified it, which includes all members of the European Union. Article 8 (1) of the Convention states 'Everyone has the right to respect for his private and family life, his home and his correspondence'.

This right to private life is not absolute and article 8 (2) exhaustively lists the possible purposes for which the right to private life can be limited: '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.'

The case law of the European Court of Human Rights (ECtHR) makes clear that the essential object of Article 8 is to protect the individual against arbitrary interference by the public authorities. There are in addition obligations on States to take positive steps to ensure that the right is respected, not merely to avoid measures which interfere with the right. In determining whether such a positive obligation exists, the Court will consider the 'fair balance that has to be struck between the general interest of the community and the interests of the individual'.

The ECtHR has held: 'Respecting the confidentiality of health data is a vital principle in the legal systems of all the Contracting Parties to the Convention. It is crucial not only to respect the sense of privacy of a patient but also to preserve his or her confidence in the medical profession and in the health services in general. Without such protection, those in need of medical assistance may be deterred from revealing such information of a personal and intimate nature as may be necessary in order to receive appropriate treatment, and, even, from seeking such assistance, thereby endangering their own health and, in the case of transmissible diseases, that of the community' (*Z v Finland* 1997; *MS v Sweden*, 1997).

The Human Rights Act 1998 (HRA98) incorporates most of the European Convention on Human rights into the domestic law of the UK. Before this anyone who thought their rights under the Convention had been violated had to make a complaint to the European Court of Human Rights in Strasbourg (ECtHR), but under the HRA98 courts in the UK can enforce some of the rights contained in the Convention. It is still open to individuals to take a case to the ECtHR in Strasbourg once they have exhausted domestic remedies.

It is unlawful for a public authority to act in a way that is incompatible with a right contained in the European Convention on Human Rights (ECHR) as set out in Schedule 1 to the Human Rights Act 1998. HSS Trusts are public bodies for this purpose and must ensure that Convention rights are not breached, both by the Trust and by its staff.

To ensure that any use or disclosure is not an interference with a service user's right to private life, any use or disclosure must serve one of the purposes listed in article 8 (2) of the ECHR. It must also be proportionate in being strictly necessary for the purpose (the aim cannot be achieved without the use or disclosure) and not represent a small benefit for a large infringement of the right to privacy.

Guidance on Human Rights Act 1998

OFMDFM, *Get in on the Act: Learning about the Human Rights Act*
http://www.ofmdfmi.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

Appendix 6: Data Protection Act 1998

The Data Protection Act 1998 (DPA98) gives effect in UK law to ‘Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data’. The aim of the Directive and thus of the DPA98 is to protect the rights of people in respect of the processing of personal data; not only their privacy rights, but all their fundamental rights insofar as they might be affected by such processing. The protections it offers only apply to ‘living individuals’.

The DPA98 introduces eight ‘Data Protection Principles’ that set out standards of information handling. The First Data Protection Principle states:

“Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless -

- a) at least one of the conditions in Schedule 2 is met, and
- b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.”

The requirement of ‘lawfulness’ means that data processing must also meet the requirements of the common law of confidentiality and the Human Rights Act 1998.

The requirement of ‘fairness’ means

The DPA98 defines ‘personal data’ as data ‘which relate to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.’

In the context of data controllers in health and social care, the most relevant Schedule 2 conditions are likely to be:

- Processing with the consent of the data subject;
- Processing necessary to protect the vital interests of the data subject;
- Processing which is necessary for the exercise of functions of a public nature exercised in the public interest by any person;
- Processing which is necessary for the purposes of the legitimate interests pursued by the data controller or those of a third party to whom the data are disclosed, except where the processing is prejudicial to the rights and freedoms or legitimate interests of the data subject.

‘Sensitive personal data’ attracts significant additional protection and is further defined in the Act to mean personal data consisting of information as to-

- (a) the racial or ethnic origin of the data subject,

- (b) his political opinions,
- (c) his religious beliefs or other beliefs of a similar nature,
- (d) whether he is a member of a trade union,
- (e) his physical or mental health or condition,
- (f) his sexual life,
- (g) the commission or alleged commission by him of any offence, or
- (h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

The most relevant Schedule 3 conditions are likely to be:

- Processing with the explicit consent of the data subject;
- Processing necessary to protect the vital interests of the data subject or another person, where it is not possible to get consent;
- Processing necessary for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings), obtaining legal advice, or is otherwise necessary for the purposes of establishing, exercising or defending legal rights;

The Information Commissioner has issued guidance on how much information it is necessary to provide to service users to meet the requirements of the DPA98. The key point is that the information provided should provide sufficient information to allow service users to exercise their rights in relation to their data under the Act. ‘They should be told who will process their data, including any disclosures of personal data (which will allow them to make subject access requests), whether it must be supplied (which will allow them to opt-out if they wish), and what information is contained in their record (which will allow them to give meaningful consent to its processing.) It should provide sufficient information to allow the individual to assess the risks to him or her in providing their data, in consenting to their wider use, in choosing not to object to their processing etc. This should have at least two consequences for data controllers. It should become clear that fair processing notices do not need to contain a large amount of detail about routine, administrative uses of data.’

It is clear that the content of health and social care records is sensitive personal data. If information does not fall under these definitions of ‘personal data’ and ‘sensitive personal data’, then the Data Protection Act 1998 does not apply. It is important to note that the data must relate to a ‘living individual’ in order for the data to be protected under the Data Protection Act.

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)

DRAFT

Appendix 7: Good practice in making discretionary disclosures in the public interest

The ‘public interest’ is not open to specific definition and its content is only conclusively determined by the courts in particular cases. Examples of purposes of intended disclosures which may be in an overriding public interest include: prevention of harm to third parties; child protection; protecting vulnerable adults; prevention of terrorism; misuse of controlled drugs; investigation of serious professional misconduct.

It is important to note that the range of public interests by which the right to private life guaranteed by Article 8 (1) of the European Convention on Human Rights (see Appendix 5) can be limited is exhaustively specified by Article 8 (2). They are: 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.

Decisions to disclose service user identifiable information outside health and social care services where no obligation to disclose information exists, are matters of balanced judgement. Factors to consider when reaching such a decision are, among others:

- 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 a sufficiently appropriate authority to whom disclosure can be considered;
- the necessity of the disclosure to avert the harm, that is, that there is no 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.

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.

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 their legal representative (see 18);
- 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 are 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 at risk.

Appendix 8: Handling Requests for Access to Personal Information

Service users have a general right to access their health and social care records. The Data Protection Act 1998 gives individuals a right of access to personal data which relates to them and is held by a data controller. These rights are known as 'subject access rights' and in exercising them a person can make a 'subject access request' to see the information held.

Under the Data Protection Act there are two possible reasons for not disclosing the requested information. In disclosing information contained in a health or social care record, care must be taken not to disclose information relating to or provided by another individual without the consent of that individual unless it is reasonable in all the circumstances to do so (this does not in general apply to information relating to a health professional involved in care provision). A key factor in assessing the reasonableness of such a disclosure is any duty of confidentiality owed to that other individual. Care must also be taken where the release of information may cause serious harm to the physical or mental health of the service user or any other person. The content of records should be assessed and any material removed necessary to avoid causing harm or breach of confidentiality.

Sometimes individuals make requests for service user information making reference to the Freedom of Information Act 2000. There is no requirement in either the Data Protection Act 1998 (DPA) or the Freedom of Information Act 2000 for an individual to make reference to these Acts in order to trigger their entitlement to access information (personal or otherwise). If the request for personal information is a request from the data subject, then the request should be dealt with under the provision of DPA. There are exemptions to the right of subject access which are contained in the DPA. Where the request relates to third party personal information, then that request must be dealt with under section 40 (ii) of the Freedom of Information Act 2000. Where disclosure to the requestor would breach any of the Data Protection principles, then such information is exempt under the Freedom of Information Act. This is a complex area and staff ought to consult the Information Commissioner's Office guidance in relation to Freedom of Information.

Further Guidance

Department of Health, *Guidance for Access to Health records Requests under the Data Protection Act 1998* (2003).

<http://www.dh.gov.uk/assetRoot/04/03/51/94/04035194.pdf>

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

http://www.dh.gov.uk/PolicyAndGuidance/InformationPolicy/PatientConfidentialityAndCaldicottGuardians/AccessHealthRecordsFAQ/fs/en?CONTENT_ID=4039714&chk=iOJNGp

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>

Appendix 8: Good practice in making decisions about information use or disclosure with service users lacking capacity

An adult has the capacity to give or withhold consent to the use or disclosure of their information if he or she can:

- a) understand and retain the information relevant to the decision in question;
- b) believe that information;
- c) weigh that information in the balance to arrive at a choice.

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:

- (a) show understanding of the idea of disclosure of confidential information about themselves;
- (b) show understanding of the possible implications of agreeing to the disclosure of information or of refusing it;
- (c) retain the information sufficiently to come to a decision;
- (d) believe the relevant information;
- (e) come to a decision;
- (f) communicate their decision.

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.

Just as with service users who have capacity, disclosure of the confidential information of a service user who lacks capacity may be in the public interest. (See 5.20-5.28)

DRAFT

Appendix 9: List of statutes prohibiting, requiring or permitting disclosure of confidential information

[The Draft England/Wales guidance directs to a website for this information—this is perhaps sufficient as very few people will need to know the whole list and anyone whose work engages with a particular statutory requirement is likely to be aware of it from other sources.]

DRAFT

Appendix 10: International Standards relevant to the protection of privacy in health and social care

As well as the protection afforded by domestic law, many instruments of international law are of relevance to the protection of the privacy and confidentiality of users of health and social services. It is important to note these for two reasons. They are often the ultimate source of the domestic law and they demonstrate the widely shared nature of the value of privacy in health and social care. Such international standards vary in their significance and provenance and include:

European Standards on Confidentiality and Privacy in Healthcare (2006)

Universal Declaration of Human Rights (1948). Article 12: ‘No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks’.

International Covenant on Civil and Political Rights (1966). This is a treaty legally binding on all European Union states. Article 17: ‘No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks’.

UN Convention on the Rights of the Child (1989). Article 16: 1. No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation. 2. The child has the right to the protection of the law against such interference or attacks.

Universal Declaration on Bioethics and Human Rights (2005). Article 9: ‘The privacy of the persons concerned and the confidentiality of their personal information should be respected. To the greatest extent possible, such information should not be used or disclosed for purposes other than those for which it was collected or consented to, consistent with international law, in particular international human rights law.’

UN Convention on the Rights of Persons with Disabilities (2007) Article 22:

“1. No person with disabilities, regardless of place of residence or living arrangements, shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence or other types of communication or to unlawful attacks on his or her honour and reputation. Persons with disabilities have the right to the protection of the law against such interference or attacks.

2. States Parties shall protect the privacy of personal, health and rehabilitation information of persons with disabilities on an equal basis with others.”

Council of Europe’s Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) (ETS n° 005, 1950 as amended).

Article 8 . Right to respect for private and family life

1 Everyone has the right to respect for his private and family life, his home and his correspondence.

2 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.

Council of Europe ‘Convention for the Protection of Human Rights and Dignity of the Human Being with Regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine’ (No. 164) (1997).

Article 10: (1) Everyone has the right to respect for private life in relation to information about his or her health. (2) Everyone is entitled to know any information collected about his or her health. However, the wishes of individuals not to be so informed shall be observed. (3) In exceptional cases, restrictions may be placed by law on the exercise of the rights contained in paragraph 2 in the interests of the patient.

Additional Protocol to the Convention on Human Rights and Biomedicine, concerning Biomedical Research (No. 195) (2005) Article 25 (1): ‘Any information of a personal nature collected during biomedical research shall be considered as confidential and treated according to the rules relating to the protection of private life.’

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* (November 2004).

<http://www.nmc-uk.org/aFramedisplay.aspx?documentID=201>

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.gsc.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 Privacy/Confidentiality for Particular Groups of Service Users

Guidance issued jointly by the BMA, GMSC, HEA, Brook Advisory Centres, FPA and RCGP, *Confidentiality and people under 16* (1994)

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

General Medical Council, *Children and Young People: Doctor's Roles and Responsibilities*

Other Relevant Guidance

'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, DHSSPS, Version 1.1 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>

Department of Health, *Guidance for Access to Health Records Requests under the Data Protection Act 1998* (2003)

http://www.dh.gov.uk/en/Policyandguidance/Informationpolicy/Patientconfidentialityandcaldicottguardians/DH_4084411

Appendix 11

PRIVACY ADVISORY COMMITTEE

Professor Roy McClelland	Belfast HSCT	Chairman
Mrs Jan Maconachie	Northern HSCT	
Dr John Jenkins	Northern HSCT	
Dr Grace Irwin	Northern HSCT	
Dr John Jenkins	Northern HSCT	
Mark Eustace	Eastern HSSB	
DHSS Representative	Mr David Reilly, Head of Information Branch	
Project Manager	Eveline Fleeton	Southeastern HSCT