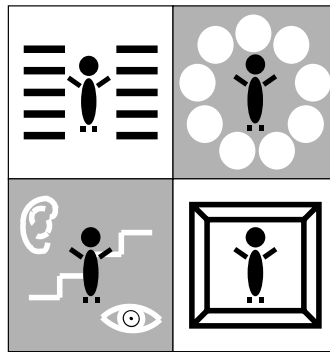


Northamptonshire Single Assessment Process



INFORMATION SHARING PROTOCOL

APRIL 2004

Northamptonshire Single Assessment Process

PROTOCOL FOR SHARING CONFIDENTIAL PERSONAL INFORMATION

APRIL 2004

LIST OF CONTENTS

SECTION	PAGE NO
Introduction	3
About the Protocol	3
Organisations who subscribe to the principles of this Protocol	4
Dates of Protocol Operation and Review	4
Definition of confidential personal information	4
Aims of the Protocol	5
Objectives of the Protocol	5
Principles of the Protocol	6
Procedural guidelines for information sharing	7
Security and Protection	8
Major Source Documents	10
Related Policies in Partner Organisations	10
Appendix 1	11
Appendix 2	13
Appendix 3	14

Introduction

1. Northamptonshire is due to implement the Single Assessment Process by 2004. This will enable multi-agency working to enable a more concise assessment process for people.
2. The protocol for sharing confidential personal information about people within the assessment process is intended to create a climate of close co-operation.
3. The protocol has been developed by a multi disciplinary team of health & social care professionals and the voluntary sector. It is a countywide group established in response to the National Service Framework for People (Department of Health) 2001. The working group developing this protocol is representative of all the Health Services, Community Services, Housing and Voluntary organisations who will enact the protocol.

About the Protocol

4. This protocol relates to confidential personal information about people in Northamptonshire who are taking part in the single assessment process. It has been developed to provide a single co-ordinated assessment for people with health and social needs.
5. The protocol has been designed to enable the exchange of confidential information and to ensure agencies do not duplicate assessments and that contributions to assessments are effective and in proportion to people's needs.
6. Consultation with user and carer groups has been an integral part of this protocol process to ensure the support received by people from family, friends, neighbours and relatives is recognised and represented.
7. Other agencies who are not party to this agreement are not covered by the protocol.
8. It must be clearly recorded if consent has been given or withdrawn to the sharing of confidential information.

Organisations who subscribe to the principles of this protocol

9. The following organisations subscribe to the principles of this protocol:

Northamptonshire Health Care NHS Trust
 Northamptonshire County Council Community Services
 Northampton General Hospital NHS Trust
 Kettering General Hospital NHS Trust
 Two Shires Ambulance NHS Trust
 Alzheimer's Society
 Age Concern
 Serve
 RNIB
 Northants Carers Association
 Northampton PCT
 Daventry & South Northants PCT
 Northamptonshire Heartlands PCT
 Northampton Borough Council
 Daventry District Council
 East Northants Council
 Corby District Council
 Kettering Borough Council
 South Northants District Council
 Borough of Wellingborough Council

Dates of Protocol Operation and Review

10. The protocol will operate from April 2004 and be reviewed April 2005
11. The protocol will be audited and reviewed in April 2005 by the Northamptonshire Single Assessment Process Implementation Group.

Definition of confidential personal information

12. Confidential personal information is:
- Any information that has been given is on the understanding that it will only be used for a specific purpose;
And/ or:
 - Any information which could lead someone to identify an individual;
And/ or:
 - Sensitive personal data such as information about an individual's physical or mental health, racial or ethnic origin, political or religious beliefs, sexual life, commission or alleged commission of any offence.

13. Confidential personal information may be recorded on paper or on electronic media and is subject to the Data Protection Act 1998.

Aims of the Protocol

14. The protocol aims to facilitate the exchange and sharing of confidential personal information in a way that is:-

- Consistent
- Respectful of the individual's right to confidentiality
- Meaningful to the person(s) requiring it
- On a need to know basis i.e. to those with a legitimate interest and appropriate level of access to the information
- With the individual's permission to share certain information with particular persons with interest i.e. information that is relevant or pertinent to the service provider

It also aims to allow the sharing of confidential information in a variety of settings:

- Within an operational unit
- Within an organisation
- With external organisations
- For non-clinical purposes e.g. analysis for monitoring of service agreements, research and evaluation, administration of an organisation and service planning

Objectives of the Protocol

15. To safeguard the service user's right to confidentiality in the sharing of information by clarifying:

- Who has access to it
- How is it used and interpreted
- What it is needed for
- How is it transferred

To safeguard professionals and legitimate others by providing guidelines that will:-

- Ensure they have enough information to make a judgement about how to proceed
- Ensure they are informed about any known or potential risks
- Allow access to confidential personal information about people within given parameters

Principles of the Protocol

16. It is not possible to legislate for all circumstances when and in what manner confidential information should be shared. For this reason the protocol operates on the basis of a series of principles which professionals should apply to each situation when making decisions about sharing confidential information

17. Principle One: Shared Records

Records (written or electronic) relating to a persons needs which are kept by parties to this agreement should be regarded as being held by the originating organisation and accessible by other organisations who are party to this agreement within the defined arrangements

18. Principle Two: General Consent

a. The person who is receiving an assessment or service through the service settings in section 9 has given general consent (verbal, non-verbal or written) for the aforementioned sharing of personal information with other parties to this agreement. This consent may be withdrawn (see 18c for details). It is essential that it is recorded that the person has been informed about the general consent principal and how they responded must be recorded

b. This consent only applies to those staff, or their managers **who need to have this information**. The need to have information relates to the assessment, provision, review of services or other statutory or authorised functions. "Need to know" is defined as follows:

The recipient of the information is or may be concerned with the person's needs and not having the information will be detrimental to the person's outcome

The use of the information can be justified for the wider purposes of ensuring and improving the quality of care and treatment, monitoring and protecting public health, effective care administration

c. The person will be made aware that to plan and provide effective care, personal information may need to pass between organisations, agencies involved and professionals on behalf of agencies. It is the assessor's responsibility to ensure that the person is informed of the consent principles of the single assessment process at the outset. The person or their advocate will be able to withdraw this consent if they specify in writing that information cannot be shared. Consent to sharing personal information can be implied if the person has been informed and does not object.

The provision of consent applies only to the disclosure of any confidential information to agencies party to this agreement. If an outside agency is providing a needs led service on behalf of the organisations listed in section 9, only relevant information should be passed on.

- d. Whilst there is a principle of consent by the person to the disclosure of information, this does not override the need to maintain confidentiality according to the principles laid down in this protocol.
- e. For further clarification about consent see Appendix 1.

19. Principle Three: Disclosure without consent under exceptional circumstances

According to the Data Protection Act 1998 where particular circumstances do occur in which disclosure of information is required/warranted, for example

- By statute or the order of the court, or
- Where there is a serious public health risk or risk of harm to the person or other individuals
- For the prevention, detection or prosecution of a serious crime

Information will be disclosed without a person's consent.

Procedural guidelines for information sharing
--

20. Dissemination of information to others:

This relates to any person assessed under the single assessment process as being high risk (using each organisation's own risk assessment criteria).

- It is the assessor's responsibility to communicate all information relating to risk to all relevant organisations/individuals using the assessment process.
- Any person other than the assessor who is involved in the care of the person and who identifies a new area of risk has a duty to update the record or inform the current service providers.

21. Requesting information from others:

This relates to an authorised person requesting information about an individual from another authorised person involved in the care of the individual.

- It is the responsibility of the requestor to clearly explain the level of urgency and risk that is attached to the request
 - Timescales for sharing of confidential information should be agreed and clearly communicated between the requestor and the person dealing with the request. Timescales should be adhered to.
 - In considering timescales there are two reasons for timely and effective information sharing: a) how the information will contribute to the quality of the service provided to the person and b) what could happen if information is not shared in an effective and timely manner and care breaks down?
22. In circumstances of disagreement or where it is unclear whether or not to disclose confidential personal information staff should contact their senior manager.

Security and Protection

23. The following points seek to provide guidelines on how to store and transfer information securely. More detailed guidance can be found for organisations subscribing to this protocol in their policies on confidentiality and security of information. These are referenced for information in paragraph 31. Further clarification regarding the sharing of information with volunteers and voluntary organisations can be found in Appendix 3.
24. Individuals should feel confident that information about them is confidentially stored and transferred, and is made available only to those who need to know.
25. Storage of Computer Records:
- Personal data held on computer systems are subject to the Data Protection Act 1998. Data access is confined to those with specified authority to view it.
 - Individual access will be password protected and access levels will be defined according to need and guard against unauthorised modification.
 - All data used for evaluative purposes will be anonymised.
26. Storage of Manual Records:
- Manual records are subject to the Data Protection Act 1998. Agencies must ensure the minimum standard of:

- Locked metal cabinets
- In a locked room
- Secure key holding
- Restricted access
- Record of access

This will reduce the probability of data being tampered with or removed.

- All data used for evaluative purposes will be anonymised where possible.
27. Transport and passing on of all confidential personal information (held on paper or in electronic media), by any means including manual transport, fax or electronic mail, should be done in a secure manner.
28. There are various risks associated with the sharing of information across services and external agencies. The main risk is that unauthorised individuals may have knowledge that they do not need, and at worse could and person's use against the subject. The best way to protect confidentiality is to minimise the likelihood of these risks occurring, and to plan for what should happen in their event. Information leaks can occur in a number of ways, either accidentally or deliberately by:
1. Obtaining information about an individual by:
 - Overhearing a conversation.
 - Gaining information by telephone, by impersonation or mistaken identity.
 2. Seeing written information, by:
 - Having access to health records or papers regarding an individual.
 - Gaining access to an office or area where papers and health records are kept.
 - Accidentally receiving misdirected post or fax about the individual. Deliberately intercepting the postal system.
 - Theft of patient health records for blackmail or misuse.
 3. Seeing information on computer about an individual either accidentally or deliberately by:
 - Being able to see a screen containing information.
 - Hacking into the computer remotely.
 - Gaining access to a computer containing the information.
 - Gaining access to information on disk.
29. Reasonable steps should be taken to secure against accidental or malicious damage or erasure

Major Source Documents

30. The following documents informed the writing of this policy:
- The Single Assessment Process DOH Guidance for Local Implementation May 2002
 - The Data Protection Act 1998
 - Protocol for Sharing Confidential Personal Information about Mental Health Users

Related Policies in Partner Organisations

31. Below is a list of other related policies in organisations who are party to this agreement:
- Kettering General Hospital NHS Trust, Confidentiality Policy
 - Northampton General Hospital NHS Trust, Information Security Policy and Procedure
 - Northamptonshire Health Support Services, Informatics Policies cover the following organisations: Daventry and South Northants PCT, Northamptonshire Heartlands PCT, Northampton PCT, Northamptonshire Healthcare NHS Trust
 - Northamptonshire County Council, Community Services, Recording with Care, procedures for Records Management and Access to Records

APPENDIX 1

DEPARTMENT OF HEALTH 12 KEY POINTS ON CONSENT: THE LAW IN ENGLAND

When do health professionals need consent from patients?

1. Before you examine, treat or care for competent adult patients you must obtain their consent.
2. Adults are always assumed to be competent unless demonstrated otherwise. If you have doubts about their competence, the question to ask is: "can this patient understand and weigh up the information needed to make this decision?" Unexpected decisions do not prove the patient is incompetent, but may indicate a need for further information or explanation.
3. Patients may be competent to make some health care decisions, even if they are not competent to make others.
4. Giving and obtaining consent is usually a process, not a one-off event. Patients can change their minds and withdraw consent at any time. If there is any doubt, you should always check that the patient still consents to your caring for or treating them.

Can children consent for themselves?

5. Before examining, treating or caring for a child, you must also seek consent. Young people aged 16 and 17 are presumed to have the competence to give consent for themselves. Younger children who understand fully what is involved in the proposed procedure can also give consent (although their parents will ideally be involved). In other cases, some-one with parental responsibility must give consent on the child's behalf, unless they cannot be reached in an emergency. If a competent child consents to treatment, a parent **cannot** over-ride that consent. Legally, a parent can consent if a competent child refuses, but it is likely that taking such a serious step will be rare.

Who is the right person to seek consent?

6. It is always best for the person actually treating the patient to seek the patient's consent. However, you may seek consent on behalf of colleagues if you are capable of performing the procedure in question, or if you have been specially trained to seek consent for that procedure.

What information should be provided?

7. People need sufficient information before they can decide whether to give their consent: for example information about the benefits and risks of the proposed treatment, and alternative treatments. If the person is not offered as much information as they reasonably need to make their decision, and in a form they can understand, their consent may not be valid.

Is the person's consent voluntary?

8. Consent must be given voluntarily: not under any form of duress or undue influence from health professionals, family or friends.

Does it matter *how* the person gives consent?

9. No: consent can be written, oral or non-verbal. A signature on a consent form does not itself prove the consent is valid – the point of the form is to record the person's decision, and also increasingly the discussions that have taken place. Your Trust or organisation may have a policy setting out when you need to obtain written consent.

Refusals of treatment

10. Competent adult patients are entitled to refuse treatment, even where it would clearly benefit their health. The only exception to this rule is where the treatment is for a mental disorder and the patient is detained under the *Mental Health Act 1983*. A competent pregnant woman may refuse any treatment, even if this would be detrimental to the fetus.

Adults who are not competent to give consent

11. **No-one** can give consent on behalf of an incompetent adult. However, you may still treat such a patient if the treatment would be in their best interests. 'Best interests' go wider than best medical interests, to include factors such as the wishes and beliefs of the patient when competent, their current wishes, their general well-being and their spiritual and religious welfare. People close to the person may be able to give you information on some of these factors. Where the person has never been competent, relatives, carers and friends may be best placed to advise on the person's needs and preferences.
12. If an incompetent person has clearly indicated in the past, while competent, that they would refuse treatment in certain circumstances (an 'advance refusal'), and those circumstances arise, you must abide by that refusal.

This summary cannot cover all situations. For more detail, consult the *Reference guide to consent for examination or treatment*, available from the NHS Response Line 08701 555 455 and at www.doh.gov.uk/consent

APPENDIX 2

These guidelines give good practice advice for what to do if a telephone call is received requesting personal information

The procedure does not preclude the use of common sense. If you know the identity of the caller, and that the patient is happy for them to have the information, then it is ok to give out information. This procedure should not be a barrier to the person having communication, but should be a protection for them. If any caller is unhappy that you cannot give them information you can state that it is policy.

APPENDIX 3

VOLUNTEERS AND VOLUNTARY ORGANISATIONS

The involvement of volunteers and voluntary organisations in the provision of health care is extensive. It is therefore important that the Caldicott Principles are put into practice in this sector. People are likely to feel less certain that information about their health care will be kept confidential where those involved are not paid employees who could stand to lose their employment in the event of serious breach of confidentiality.

It is important, therefore, that where services are provided by corporate voluntary organisations, those bodies are subject to a service contract which specifically includes clauses about the maintenance of confidentiality.

The organisations may be legally obliged to register processing of data with the Information Commissioner (where data are processed on computer) and their status as a data controller under the Data Protection Act 1998 (DPA) is clear since they have control over the purposes and manner in which the data are processed. It follows that the organisations consequently have a duty to train their volunteers to appreciate the legal requirements of the DPA and the common law of confidentiality, in particular their individual culpability.

Under the legislation, it is a requirement that people are given information about the sharing of information with volunteers or voluntary agencies as a routine on collection of data, or at least prior to such sharing.

All the principles expressed in this protocol apply to volunteers, whether working for voluntary organisations or directly for health or other partner organisations, although the responsibility for training the volunteers in the latter case naturally falls to those organisations.

The method of sharing information between health bodies and voluntary organisations may be expressed in the contract between them. The transfer of information may be specified as only to be authorised via a paid organiser or administrator, but in some circumstances this will be impracticable. This process may involve additional steps of verification to establish "need to know".