NORTH WEST PUBLIC AUTHORITIES AND PARTNERS INFORMATION SHARING CODE OF PRACTICE

Legislation and Standards for Information Sharing

(Tier 1)

2011

Contents

1. Tiered Framework of the Information Sharing Code of Practice

This Overarching Standard for Information Sharing is designed to be used in conjunction with a set of documents within a Tiered Structure. The structure is designed to provide a framework for the secure and confidential sharing of information between the partner organisations that contribute to the wellbeing of residents and ensuring disclosure is in line with statutory requirements.

Information may be stored in many different formats such as, physical, electronic, audio or video.

There are 3 main tiers to the structure.-

- **Tier Zero**- This is a document signed by a Chief Executive of an organisation agreeing in principle to share information responsibly. The names of all agencies in agreement are listed and can be added to as more agencies became involved. Organisations should, if possible, place copies of tier 0 and tier 1, and a list of partner organisations, on their internet sites to reassure the public of their commitment to sharing responsibly. If not this Tier 0 document, then a document similar to a Tier 0 document must be signed by the Chief Executive of all organisations wishing to take part. Only one Tier 0 document need be signed by the Chief Executive for any number of Tier 2 documents agreed beneath it.

- **Tier One**- This is an overarching standard outlining the agreed procedures for sharing information. It is this document which sets the standards for obtaining, recording, holding, using and sharing of information.

  - Outlines the supporting legislation, guidelines and documents which govern information sharing between partner organisations

- **Tier Two**- This gives guidance to operational practitioners on the production of a protocol for the safe sharing of information. These protocols should show what information should be shared and how, under what circumstances and by whom, and should be tailored to individual partnerships. This document will require authorisation of the participating partnership organisations.

  A copy of this document should be lodged with the Information Governance section. Guidance would suggest that the following are included -

    - Fair processing notices,
    - Consent leaflets,
    - Social Care Record Guarantee,
    - Confidentiality statement,
    - Subject access
    - Privacy Impact Assessments

This Code of Practice is designed to simplify and strengthen the sharing of information between partner organisations in the North West, along with other partners which border the geographical area and with whom we may share information.

2. Purpose of the Code of Practice

The purpose of the Code of Practice is to support public service organisations and their partners in delivering holistic and responsive services. It concerns the sharing of personal data and seeks to lay the foundation for the safe and secure sharing of information in order to comply with the duties placed on organisations to work together. As such, it is intended as a means of establishing a standard to which all Partner Organisations will work towards in respect of the treatment of personal information.

The Code of Practice has a contribution to make towards fostering a culture in which all services work together to deliver better outcomes for the residents and visitors in the North West of England. The objectives of the Code of Practice are:

- To assist staff in protecting the confidentiality of patients, clients and employees where it is necessary to share personal data.

- To help local partnerships by providing a secure and efficient way to exchange personal data where a power exists to do so, in accordance with the Data Protection Act 1998, the Human Rights Act 1998 and other relevant legislation.

- To support joined up local services.

- To promote good practice in data sharing, with regard to general management, data quality, etc.

Each Partner Organisation has its own local policies and procedures regarding information security and confidentiality. This Code of Practice is not designed to supersede existing local policies but to enhance them by facilitating cross-boundary dialogue and agreement and providing a context for Information Sharing between organisations within the North West.

3. Commitments to Service Users given through the Code of Practice

The Code of Practice is a sign of our commitment and a demonstration to the public about how information is used and our statement to the population of the North West is:

We will:

- Ask for permission to collect and share your information, and where you have a choice as to whether to provide us with information, we will make it as easy as possible for you to exercise that choice.
- Explain why we are using your information, and will only use it for those purposes.
- Explain who will see it, and limit access to your information only to staff who need it.
- Only ask for information we need, and not ask for information which is not relevant to your needs/our service.
- Keep information about you as accurate and up-to-date as possible – with your help.
- Respect your rights under the Data Protection Act 1998 – including your right to see the information which has been recorded about you.
- Protect your information with the highest possible standards of security and confidentiality.
- Tell you how you can get more information, including:

    How we safeguard your personal information;
    How you can check and correct any information we hold;
    How to raise a query or a complaint.

- Only keep the information for as long as needed, and explain our reasons when we need to keep personal records for some time after we have stopped providing a service to you. This is usually so that we can resume a service at a later date if needed.

4. Roles and responsibilities

4.1 Partner Organisations who are signatories to the Code of Practice

Partner organisations who are signatories to this Code of Practice will:

- Promote staff awareness of the requirements around information sharing, through training, issuing of guidelines, etc.
- Have in place appropriate internal information governance and/or operational policies and procedures that will facilitate the effective processing of personal information which is relevant to the needs of the organisation, their managers/practitioners and their service users.
- Ensure that their organisational and security measures are moving towards compliance with BS ISO/IEC 2700 series (see page 10), to protect the lawful use of information shared under this Code of Practice.
- Comply with the security levels on supplied information and handle the information accordingly.
- Ensure that all appropriate staff have the necessary level of CRB clearance in accordance with relevant legislation and Government guidance, as required by each protocol under this Code of Practice.
- Accept responsibility for independently or jointly auditing compliance with the individual protocols they are involved in.
- Accept responsibility for ensuring that any information which is obtained under the auspices of this Code of Practice is not used for marketing purposes unless appropriate consent has been obtained
- Only use the information for the purpose for which it has been shared.
- Take all reasonable actions to ensure that information provided under the auspices of this Code of Practice is, and remains accurate.
- Where there is reason to believe that a record may be inaccurate, investigate to rectify the record, or advise the record owner from whom the record was obtained so that they may investigate/rectify.
- Ensure contracts with contractors include the relevant clauses regarding confidentiality, information security and completion of the relevant Information Governance Toolkit.

Each Partner organisation will nominate a lead officer for the purposes of monitoring, reviewing and developing this Code of Practice, hosted by the Lancashire and Cumbria Information Governance Group.

4.2 The role of the Lead officer

The Information Governance lead officer for each Partner Organisation will act as lead or main contact point for communication and dissemination purposes, internal information governance and/or operational procedures and processes. The lead officers collectively will facilitate the dissemination and implementation of, and monitoring and

evaluating adherence to, the Code of Practice within their organisations. This will include future development of the Code of Practice.

4.3 The role of the Review Group

The Lancashire and Cumbria Information Governance Group comprising of lead officers from each Partner Organisation will be the Review Group. The group will discuss issues, share good practice, collaborate on policy development, monitor adherence, and make recommendations for future development, policies, etc.

5. Service protocols supporting the Code of Practice

For each service where data sharing is a key requirement, the operational guidance document/protocol will be agreed (Tier 2).

Each protocol adopted under this Code of Practice will include explicit consideration of the policy and legislative issues which are deemed to apply to that service.

It is consistent with good practice that similar protocols should be used in support of the sharing of any data. However, it is recognised that different arrangements are required to support the sharing of personal data, compared with non-personal data. This Code of Practice encourages, but does not require protocols for the purposes of sharing non-personal data.

The absence of a protocol should not in itself be a barrier to sharing personal information.

6. Monitor and review

The Review Group will 'own' the Code of Practice on behalf of the Partner Organisations. Any party to the protocol can request reviews at any stage, eg. to address particular issues which may arise, and as a minimum, it will be reviewed every two years by the Review Group. That Group will have responsibility for updating documents to reflect changes in policy or legislation. In doing so, the Group will need to take into account what reporting arrangements would be appropriate for the amendments. There are two categories:

- Minor changes of detail can be signed off by the Group;
- Changes which require the issuing of a new Code of Practice to be signed by all Partners.

7. Signatories to the Code of Practice

By signing the Tier 0 Commitment to the North West Public Authorities and Partners Information Sharing Code of Practice all parties agree to the standards as laid down in this Tier 1 document.

8 Key Legislation and Guidance

The following is meant as guidance to some of the legislation which supports the sharing of personal data. It should not be regarded as comprehensive and when sharing personal data it is the responsibility of each organisation to ensure that sharing is lawful.

1. **The Data Protection Act 1998** represents the key legislation governing the protection and use of personal data about living, identifiable people. This legislation requires organisations to ensure any 'processing' of personal data complies with the Principles of the Act. This includes the implications of any information sharing arrangements; with particular regard for the purpose(s) information is shared. Link to Information Commissioner's Office website:
http://www.ico.gov.uk/for_organisations/data_protection.aspx

THE DATA PROTECTION PRINCIPLES (SUMMARY)

The following principles must be applied to all processing of personal data:

1. Personal data shall be processed fairly and lawfully.
2. Personal shall be obtained for only one or more specified and lawful purposes.
3. Personal data shall be adequate, relevant and not excessive.
4. Personal data shall be accurate and where necessary, kept up to date.
5. Personal data shall not be kept longer than is necessary.
6. Personal data shall be processed in accordance with the rights of data subjects.
7. Appropriate technical and organisational measures shall be taken to make personal data secure.
8. Personal data shall not be transferred to countries outside of the European Economic Area unless those countries ensure an adequate level of protection for that data.

2. **The Crime & Disorder Act 1998** introduced measures to reduce crime and disorder by introducing local crime partnerships. These were based around local authority boundaries to 'formulate and implement' strategies for reducing crime and disorder in the local area. The Act facilitates information sharing by providing agencies with the power to lawfully disclose information for the purposes of the Act. It does not, however, impose a *requirement* to exchange information. Link to legislation:
http://www.legislation.gov.uk/ukpga/1998/37/contents

   Schedule 9(5) of the Police and Justice Act strengthens this by introducing a new duty on the same agencies. This duty (section 17A) requires the sharing of depersonalised data, already held in a depersonalised format, for the purposes of reducing crime and disorder. Link to legislation:
http://www.legislation.gov.uk/ukpga/2006/48/schedule/9

3. **The Human Rights Act 1998** states (in Article 8.1) that 'everyone has the right to respect for his private and family life, his home and his correspondence'. Agencies entering into information sharing must be aware of the implications of the rights granted to individuals by this legislation. Link to legislation: http://www.legislation.gov.uk/ukpga/1998/42/contents

4. **The Common Law Duty of Confidence**. When considering personal information that has been provided 'in confidence', then all staff of any organisation with access to such information are subject to the Common Law Duty of Confidence. This duty is recognition, in law, of the need to ensure that the information remains confidential. All health information so provided, within any of the partner

organisations, imposes such a duty on staff who have access to the information. Link to website archive for NHS information explaining the Common Law Duty of Confidence: http://www.legislation.gov.uk/ukpga/1998/42/contents

5. **The National Health Service Act 2006** allows the processing of patient identifiable information, without consent, for certain limited purposes when agreed by the Secretary of State for Health, where there are real barriers to seeking or obtaining consent. This legislation, however, is viewed as an interim solution to facilitate certain information sharing until robust methods of obtaining express, informed consent for all sharing have been developed. Link to legislation website: http://www.legislation.gov.uk/ukpga/2006/41/contents

6. **The Freedom of Information Act 2000** gives a general right to access to all types of recorded information held by Public Authorities, except personal data. It gives the public the right to be told if the information exists and; the right to receive that information. Agencies entering into information sharing arrangements must be aware of the rights granted to individuals under the Act and ensure that personal data, where covered by exemptions defined in the act are not disclosed. Link to Information Commissioner's Office website: http://www.ico.gov.uk/for_organisations/freedom_of_information.aspx

7. **The Children Act 1989** places specific duties on agencies to co-operate in the interests of vulnerable children. These duties are also highlighted in the **Children Act (2004).** The Children Act 1989 places a statutory duty on Health and Social Care Professionals to help each other with their enquires so long as it is compatible with their own statutory duties or other duties and obligations. Link to Department for Education website: http://www.education.gov.uk/publications/standard/Childrenandfamilies/Page1

8. **Confidentiality: NHS Code of Practice**" published by the Department of Health in November 2003 and endorsed by the Information Commissioner, General Medical Council (GMC), British Medical Association (BMA) and Medical Research Council provides guidance in relation to the sharing of confidential information. Confidential Patient information generally should not be passed to non-NHS bodies, although there are exceptions where it can be. Link to Department of Health: www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4069253

9. **Caldicott Principals** NHS & Social Care organisations that are parties to this General Agreement must recognise the requirements and be committed to the principal recommendations of the Caldicott Committee Report. These recommendations, published in December 1997, included the requirement to develop local 'inter-agency' information sharing protocols. Link to Department of Health website: www.dh.gov.uk/en/publicationsandstatistics/publications/publicationspolicyandguidancwe/dh_4068403

The six Caldicott Principles summary:

1. Justify the purpose – i.e. there has to be a legitimate reason for the transfer of the data.
2. Don't use personal identifiable information unless it is absolutely necessary.
3. Use the minimum necessary personal identifiable information.
4. Access to personal identifiable information should be on a strict need to know basis.
5. Every one with access to personal identifiable information should be aware of their responsibilities.
6. Understand and comply with the law.

10. **British Standard ISO/IEC 27002 (ISO17799/BS7799)** NHS organisations and other public organisations that are parties to this General Agreement currently work on the principles of the

Information Security Standard British Standard ISO/IEC 17799 (BS 7799). Recommendations include procedures when exchanging information. Social Care & Non – NHS organisations who are parties to this General Agreement must recognise the requirements of this Standard and ensure that information sharing takes place in a manner compatible with those requirements. Link to BSI website: www.bsi-emea.com/InformationSecurity/Overview/Whatare+ISO27001+27002.xalter

11. **Information Governance Toolkit** NHS and various other Organisations are required to adopt the Information Governance Toolkit which is a knowledge base and assessment framework. The toolkit brings together in one place information and activities to support the provision of high quality care. It promotes the effective and appropriate use of information with an increased importance of data sharing and partnerships. Link to Department of Health Information Governance Toolkit website: https://nww.igt.connectingforhealth.nhs.uk/

12. **The Laming Report (2003),** Every Child Matters (2003) highlights the importance of safeguarding all children by effective communication highlighting the areas of:

    - Multi-agency partnerships and information sharing.
    - A common assessment framework.
    - Accountability
    -

    Detailed guidance regarding information sharing for the purposes of safeguarding and promoting the welfare of children is available in 'What to do if you're worried a child is being abused' (DOH 2003). Link to Department of Health website: www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4008654

13. **Social Security Administration Act 1992.** Under section 123 of the Social Security Administration Act 1992, it is a criminal offence for anyone who is or was engaged in any aspect of social security administration to disclose information obtained through such activity without lawful authority. Partnership members must be made aware that any unauthorised disclosure may lead to criminal proceedings against them. Link to legislation: http://www.legislation.gov.uk/ukpga/1992/5/contents/enacted

Mental Capacity Act 2005
http://www.opsi.gov.uk/ACTS/acts2005/ukpga_20050009_en_1

Criminal Justice and Immigration Act 2008
http://www.opsi.gov.uk/acts/acts2008/ukpga_20080004_en_1

NHS Act 2006 Section 251
http://www.opsi.gov.uk/Acts/acts2006/ukpga_20060041_en_1

Government Connect. http://www.govconnect.gov.uk/

Information Commissioner's website http://www.ico.gov.uk/

NIGB http://www.nigb.nhs.uk/

Education Act http://www.opsi.gov.uk/ACTS/acts2005/ukpga_20050018_en_1