Department of
Health, Social Services
and Public Safety
www.dhsspsni.gov.uk

DHSSPS & HSC PROTOCOL FOR SHARING SERVICE USER INFORMATION FOR SECONDARY PURPOSES

Document Status

The current status of this document is: Draft

Version History

Number of this Version: 5
Date of this Version: August 2011
Date for Review: August 2012

Previous Version Number & Date	
1 October 2009	***Changes following consultation with Personal Data Guardians.***
2 November 2009	***Changes following consultation with Privacy Advisory Committee, Information Governance Advisory Group, Information Governance Project Board Rep and Departmental Solicitors Office.***
3 December 2009	***Changes made during final consultation before protocol sign off.***
4 July 2011	***Changes following Review.***

CONTENTS

Part 1

Why We Need An Information Sharing Protocol

This protocol should be read in conjunction with the Code of Practice on Protecting the Confidentiality of Service User Information (which will hereby be referred to as the Code of Practice), launched by the Department in January 2009. The Code of Practice provides detailed guidance on all aspects of protecting the confidentiality of service user information.[1]

Introduction

1.1 Government policy places a strong emphasis on the need to share relevant personal information across organisational and professional boundaries, in order to ensure effective co-ordination and integration of public services. It also emphasises the importance of security and confidentiality in relation to personal information.

1.2 Current practice across the Health & Social Care (HSC) family, in relation to information sharing, varies considerably. Some staff may be reluctant to share personal information about service users because of uncertainties about current guidance. This can lead to serious difficulties in ensuring that services are properly co-ordinated.

1.3 Other staff may be unaware of the implications of recent developments, such as the launch of the Code of Practice, and may be continuing to share information on the basis of informal arrangements. These arrangements may not comply with the current Code of Practice, leaving individuals and the bodies they work for open to scrutiny and challenge. [2]

1.4 The aim of this protocol is to further support and embed the principles and guidelines of the Code of Practice and to assist the Department of Health,

[1] The Code of Practice is available at, http://www.dhsspsni.gov.uk/confidentiality-code-of-practice0109.pdf

[2] In January 2009 the Department of Health, Social Services and Public Safety (DHSSPS), launched the Code of Practice to, "…provide support and guidance, for all those involved in health and social care, concerning decisions about the protection, use and disclosure of service user information." (*From the Foreword by DHSSPS Permanent Secretary, Andrew McCormick, 'Code of Practice on Protecting the Confidentiality of Service User Information', January 2009.*)

Social Services and Public Safety (DHSSPS), HSC and Public Safety bodies to comply with the Code of Practice. (For the purposes of this protocol the Department, HSC and Public Safety bodies covered by the protocol will be referred to as 'partner organisations.')[3]

1.5 The protocol should assist partner organisations in establishing 'on the ground' procedures for sharing data between them and in developing specific Data Access Agreements. A standard Data Access Agreement template has been developed in line with the requirements of this protocol.

1.6 The protocol focuses on the sharing of information about service users for secondary uses or purposes. This includes the sharing of service user identifiable information, in relation to which the Code of Practice defines secondary uses as the "…**disclosure of personal identifiable information for purposes of health and social care not directly related to the care of that service user.**"[4] Examples of secondary uses are provided in the Code of Practice, (Para 3.14); these include sharing personal identifiable information for 'planning purposes', 'auditing accounts' and 'public health monitoring'.

1.7 The protocol should be seen as a resource that will help support staff when making decisions about information sharing, as it should help promote best practice and ensure a consistent approach to information sharing across the HSC sector in Northern Ireland (NI).

1.8 This protocol has been developed by a Strand Team, led by the DHSSPS' Departmental Information Manager, consisting of representatives across the Department, Trusts and Non Departmental Public Bodies (NDPBs). Consultation took place before the final version of the protocol was produced. Consultees included:

[3] A list of Partner Organisations is provided at Appendix 3.
[4] Paragraph 3.2(B) of the Code of Practice.

- Personal Data Guardians (PDGs).[5]
- Information Governance Advisory Group (IGAG).
- Privacy Advisory Committee (PAC)
- DHSSPS Representative of the Information Governance Project Board.

1.9 The protocol was developed in line with guidance from the Information Commissioner's Office (ICO), including 'The Framework Code of Practice for Sharing Personal Information' and 'Sharing Personal Information: ICO Approach'. It has recently been reviewed in line with the publication of the ICO's 'Data Sharing Code of Practice' (May 2011).[6]

Service User Consent & Legislative Requirements

1.10 The Code of Practice sets out the approach to be taken when considering service user consent, in relation to the processing, disclosure or sharing of their personal information.[7] The basic advice is, "if the service user refuses to consent to the disclosure of personal information, the information cannot be disclosed, unless, exceptionally, a justification other than consent exists."[8]

1.11 In relation to consent and the use of personal information for secondary uses, the Code of Practice specifically advises that "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."[9] The only exceptions to this approach are where there are legal or statutory grounds for disclosure, or where there is an 'over-riding public interest', which clearly outweighs the public interest in maintaining confidentiality. Further guidance, for example about considering the public interest and examples of cases when staff may need to disclose personal

[5] The Patient and Client Council (PCC), which represents patients, clients and carers, were involved in this consultation via their PDG.
[6] All ICO Guidance can be found on the ICO website- www.ico.gov.uk
[7] See paragraphs 2.6 – 2.8 of the Code of Practice.
[8] Code of Practice, paragraph 2.7.
[9] Code of Practice, paragraph 3.16.

information for secondary uses or other purposes, is available within the Code of Practice.[10] Staff should also use the flow diagram provided within the Code of Practice, (included at Appendix 5 of this protocol), which covers 'the key considerations in making good decisions about the use and disclosure of identifiable service user information' in this context.

1.12 As noted in the Code of Practice[11], in NI there is no equivalent to section 251 ('Control of patient information') of the National Health Service Act 2006, which states,

"(1) The Secretary of State may by regulations make such provision for and in connection with requiring or regulating the processing of prescribed patient information for medical purposes as he considers necessary or expedient—
(a) in the interests of improving patient care, or
(b) in the public interest."[12]

1.13 The Department is currently giving consideration to the introduction of legal support for non-consented use of service user identifiable information. Without this legislation in place in Northern Ireland, it is important to recognise that any sharing of information without the patient's consent could be open to legal action under the common law duty of confidentiality. In sharing information without consent, HSC bodies/ organisations and the Department need to feel confident in the public interest test judgements and arguments they make for the disclosure and sharing of service user identifiable information. This will involve the exercise of judgement and balancing the rights of patients against the public good. The more sensitive the information, the stronger the public interest in disclosure will need to be. It is important that these judgements are taken and approved at an appropriate level and that the decisions made and evidence to support them is recorded. In some

[10] Code of Practice, paragraphs 3.18 – 3.30.
[11] Code of Practice, page 5.
[12] See http://www.opsi.gov.uk/Acts/acts2006/ukpga_20060041_en_19#pt13-pb4-l1g251

cases this may require seeking legal advice/guidance before the information is shared.

1.14 There are specific legislative requirements in relation to organisations' obligations under the Data Protection Act (DPA) 1998.[13] There are 8 DPA Principles which organisations must adhere to.[14] Of key consideration is the 1st principle which requires that all personal data is processed 'fairly' and 'lawfully'. **Any processing, including sharing, of service user identifiable information must be lawful** and the Department and HSC bodies must ensure they have the '*ultra vires'* (legal powers) to process the information for the purposes intended. An organisation/ Data Controller 'may only act within the limits of its legal powers'.[15]

1.15 The Information Commissioner has pointed out 'a common misconception… that the DPA always requires the consent of data subjects to the processing of their data'.[16] However the ICO advise that in relation to lawfulness of data processing the key issue for processing of health data is likely to be the common law duty of confidence, as "even though the (DP) Act does not explicitly require the consent of patients in order to process medical data, in many cases there is an implied requirement to obtain patient consent for the processing of data since to process without consent would involve a breach of the duty of confidence which, in turn, would involve a breach of the requirement in the Act to process personal data lawfully."[17]

1.16 Organisations are advised to develop internal procedures to help ensure that decisions to share information without consent have been fully considered and

[13] Further guidance in relation to DPA is provided in Part 7.
[14] See Appendix 4.
[15] IC Guidance, ''Use and Disclosure of Health Data: Guidance on the Application of the DPA 1998' (May 2002), page 11.
[16] Information Commissioner's Foreword, 'Use and Disclosure of Health Data: Guidance on the Application of the DPA 1998' (May 2002).
[17] IC Guidance, ''Use and Disclosure of Health Data: Guidance on the Application of the DPA 1998' (May 2002), page 11.

are compliant with the requirements of legislation. ***Further guidance on relevant legislation is included in Part 7.***

Scope/ Purpose of the Protocol

1.17 This protocol forms an agreement between the Department, HSC and Public Safety bodies/organisations listed at Appendix 3, to govern the sharing of service user information and to facilitate the development of Data Access Agreements.

1.18 For the purposes of this protocol these organisations will be referred to as 'partner organisations'.

1.19 The protocol:

- Provides a framework for sharing personal information about service users between partner organisations in Northern Ireland, which is in line with the Code of Practice.
- Includes purposes for sharing information.
- Provides practical guidance, including monitoring and review of the protocol, and dealing with protocol breaches.
- Outlines the legislation and the principles that need to underpin the information sharing process.

1.20 The benefits of the protocol include:

- Promotion of information sharing between appropriate organisations to ensure service users receive high-level, integrated services.
- Helping to ensure compliance with legislation and guidance. (The 1998 Data Protection Act stipulates that organisations must satisfy themselves that the agencies they share information with have the necessary procedures in place to comply with the Act's requirements. Partner organisations have signed up to the protocol, confirmed that they will

comply with these procedures whenever information is shared and will abide by the monitoring arrangements within the protocol.)

- Managers and operational staff are informed of the reasons why personal information about service users may need to be shared and how this sharing should be managed.
- In following the protocol, partner organisations should be able to ensure that data is only retained for as long as business or legislation requires and is disposed of in line with proper Records Management procedures and Information Security guidelines.

1.21 The protocol will be activated through Data Access Agreements (DAAs), for specific service areas, between organisations. Each DAA should set out the detailed arrangements relevant to that particular agreement. All agreements will need to be fully compliant and consistent with the Code of Practice and this protocol. A DAA Framework is provided at Appendix 2.

1.22 The protocol is not contractually binding but is to be used to set good practice standards that parties need to meet in order to fulfil any duty of care which exists in relation to the sharing of service user information.

Purposes for which Information may be shared for Secondary Uses

1.23 As noted, personal information about service users and their family/relatives can only be shared for specified, justified and lawful purposes. Some examples of why this information may need to be shared for secondary uses/ purposes may include:

- To support effective care and treatment.
- To support the monitoring of care and treatment against existing standards and benchmarks.
- To support the effective administration, audit and inspection of services.
- Risk management.

- Monitoring and protecting public health.
- Investigating complaints, incidents and notified or potential legal claims.
- Managing and planning services.
- Contracting for services.
- Statistical analysis and reporting.
- To ensure the holistic assessment of vulnerable adults' and children's development needs.
- In relation to carers.

1.24 Some purposes may require additional safeguards to be specified, e.g. research that directly involves an individual should only proceed with the individual's informed and explicit consent. Partner organisations must also ensure approval has been obtained by the researcher, from the Research Ethics Committee (NI), prior to releasing information for research purposes.

Reasons for and Benefits of Information Sharing

1.25 Information sharing:

- Helps facilitate organisations in meeting their responsibilities to protect, support and care for individuals and communities.
- Improves the effectiveness, efficiency, safety and quality of health and social care services.
- Ensures health inequalities are tackled, with the aim of improving services, without compromising the confidentiality and integrity of person/patient identifiable information.

Part 2

Document Information

Protocol Launch

2.1 This protocol has been quality assured by the Information Governance Advisory Group (IGAG), the Privacy Advisory Committee (PAC), Personal Data Guardians (PDGs) and the DHSSPS representative of the Information Governance Project Board.

2.2 The protocol was formally launched by the DHSSPS Permanent Secretary and issued to HSC Chief Executives within all partner organisations in November 2011.[18]

Protocol Administration

2.3 This protocol will be:

- Owned by the Personal Data Guardians of each of the partner organisations, who will be responsible for all amendments.
- Date and version controlled.
- Reviewed by Personal Data Guardians annually.
- Published as part of the publication schemes of all partner organisations.

Partner Organisations

2.4 The protocol requires each partner organisation to have a nominated senior professional, which should be a Personal Data Guardian (where possible), who is responsible for:

- Approving who in their organisation has access to the shared information;
- Approving amendments to the protocol;
- Ensuring mechanisms are in place to monitor its operation and ensure compliance;
- Report to relevant parties on any breaches and action taken.[19]

[18] A current list of the partner organisations covered by this protocol is provided at Appendix 3.
[19] While the Personal Data Guardian has overall responsibility for this work, it is appreciated that elements of this work may be delegated to appropriate trained staff.

Part 3

Implementing the Protocol

3.1 To ensure the successful implementation of the protocol across all partner organisations, organisations must agree to:

- Implement the protocol fully.
- Set out internal arrangements to support the protocol and ensure that staff adhere to these arrangements.
- Provide appropriate training to staff (see paras 3.14 – 3.15).
- Provide assurances to the Department, via the Controls Assurance Standard, that the protocol has been implemented within their organisation.
- Where the sharing of information is lawful, ensure through mutual agreement that information sharing is fully supported and facilitated to support the work of partner organisations.
- Ensure that Data Access Agreements are consistent with this protocol.

Disseminating the Protocol

3.2 All bodies should ensure that this protocol is appropriately implemented and communicated throughout their organisation.

3.3 The protocol should be made available internally via staff management guidance and the organisation's Intranet, or similar communication platform.

3.4 All partner organisations should make the protocol available to service users, carers and the general public via their organisational websites and publication schemes.

Outline Procedure for Use of Data Access Agreements (DAAs)

3.5 A Data Access Agreement is a specific agreement for a particular service area. This is drawn up by two or more bodies that need to share service user identifiable information.

3.6 A Data Access Agreement Framework is provided at Appendix 2. This should be used by partner organisations to develop Data Access Agreements that meet their specific data sharing arrangements.

3.7 As part of DAAs, justification for retaining patient identifiable information beyond 12 months will need to be provided and organisations should be encouraged to describe within DAAs how they will destroy the shared information once their use of this information is complete. They must also notify the originating organisation once the data has been destroyed.

3.8 It is recommended that DAAs are used by all partner organisations to manage the data sharing process. Any organisation wishing to access data from another organisation should be requested to apply to that organisation, providing the relevant information, as set out in the Data Access Agreement Framework. This information should then enable a decision to be taken as to whether or not the information should be shared.

3.9 Any DAA can only be approved by the Personal Data Guardian for the body who owns the information, or by an equivalent officer of the same seniority within the body, or by an officer with delegated authority, who must have an awareness of the information in question, as well as issues around protecting personal data and confidentiality. This will ensure that disclosure of information is only authorised, in each partner body, by an appropriate, approved officer.

3.10 The authorisation process must be documented.

3.11 Partner organisations should keep an up-to-date list of authorising officers and their contact details.

3.12 Partner organisations may develop more detailed procedures for the use of Data Access Agreements within their organisation, if required.

3.13 If there is any doubt about whether information should be stored, disclosed, or collected, staff should speak to their Personal Data Guardian, Data Protection Officer or Information Management specialist.

Training

3.14 The success of the protocol will depend upon visible high level support from senior managers within each partner organisation. Partner organisations should be committed to raising awareness of this protocol through training. They should ensure that relevant staff receive appropriate training, particularly those who are required to make decisions about data sharing. Adequate resources should be put in place to ensure that training can be provided.

3.15 At operational level staff must be made aware of internal procedures relating to data sharing. Procedures should be fully documented and disseminated to ensure that they can be followed by staff consistently.

Part 4

Monitor and Review

4.1 Personal Data Guardians (or equivalent) within each partner organisation have overall responsibility for ensuring that monitoring and review of the protocol and associated Data Access Agreements takes place. This will include ensuring that relevant staff investigate any complaints or breaches of the protocol, or DAAs, and that these are reported to the Department as part of the Controls Assurance process.

4.2 Reviews should be carried out annually. Reviews may include Personal Data Guardians asking for feedback from relevant parties within their organisation, as to how the protocol has been working and any problems that may have arisen either in relation to the protocol, or to any Data Access Agreements. Feedback may also include proposed amendments to the protocol.

4.3 As part of the review process, Personal Data Guardians should meet annually to discuss any issues and proposed amendments to the protocol so that these can be taken forward. They should also use this opportunity to discuss and share any lessons learned in relation to data sharing. The Information Governance Advisory Group will co-ordinate this annual meeting of Personal Data Guardians, though Personal Data Guardians should aim to communicate, liaise and network with their counterparts in other bodies on an ongoing basis.

Part 5
Complaints and Disciplinary

5.1 Complaints about the use of personal information or breaches of the protocol will be dealt with under the relevant complaints procedure of the partner organisation where the complaint/breach was raised. If the complaint affects more than one partner organisation, it should be brought to the attention of the appropriate officers within that organisation, so that the complaint/breach can be fully investigated. All breaches will need to be recorded, investigated and the findings noted.

5.2 Complaints or breaches may be reported by staff or members of the public. Staff will follow their normal internal procedures for reporting breaches or complaints. If an organisation receives a complaint from a member of the public, this should be investigated in accordance with their complaints policy and procedures.

5.3 For partner organisations that adhere to the Regional Adverse Incident and Learning (RAIL) System (as outlined in Circular HSC (SQSD) 22/2009), adverse incidents should be reported to the HSC Board and Public Health Agency (PHA). Partner organisations should also notify the Department, via the Early Alert System, of any event which has occurred, which meets one or more of the seven criteria set out in the Early Alert System (as outlined in Circular HSC (SQSD) 10/2010).

5.4 Staff who may need to be notified of complaints/breaches include:

- Personal Data Guardians (PDG).
- Data Protection Officers (DPO).
- Data Security Officers (the Assistant Departmental Security Officer (ADSO) in the case of the Department).
- Information Management staff.

5.5 Personal Data Guardians (or equivalent), from partner organisations, should meet annually to:

- share good practice and review any reported breaches of the policy; and
- update the protocol, either where the reported breaches indicate the need for change to be made, or where general improvements are agreed.

5.6 Every partner organisation should publish their procedures for handling data sharing complaints and staff should be adequately trained to deal with complaints.

5.7 Procedures should cover disciplinary action which may be taken against any member of staff who does not fully adhere to the organisation's policies and procedures. Disciplinary action may cover instances where a member of staff has:

- Accessed data without appropriate authorisation; or
- Disclosed data without authorisation.

Part 6

Important Information Governance Considerations

Quality of Information is Assured and Maintained

6.1 Partner organisations must be able to ensure the quality of information they hold. This includes ensuring information is factually correct, up-to-date and, where errors are found, that these are corrected, not only by the originating body but across any organisations with which the information has been shared. Particular care is required to ensure accuracy where any type of data matching exercise has/is taking place.

6.2 Data sharing arrangements should be regularly reviewed to ensure that the information shared continues to be for lawful, necessary and justifiable purposes and continues to be relevant and not excessive for the purposes identified.

Electronic Data Sharing and Databases

6.3 Where partner organisations use or develop a database to share pooled data, they must establish which organisation will be the 'data controller' for that database. The 'data controller' will be responsible for establishing who should have access to the database and on what basis. They must also consider which parts of the database staff should have access to and should restrict staff access to the appropriate information accordingly. They should consider what information could be anonymised or pseudonymised and which staff should be authorised to access person identifiable information or the keys/codes to anonymised or pseudonymised data, which should be strictly limited.

6.4 Staff will need to know the standards for entering personal information on a database or on manual files so that there is consistency in the format of the data that is shared.

6.5 All databases must comply with the original purposes for which they were established, which in turn should be compliant with relevant legislation.

Access & Security

6.6 In line with Principle 7 of the DPA1998, partner organisations must put in place appropriate technical and organisational measures to protect personal information. This should include clearly setting out the technical and organisational security arrangements that are in place for protecting shared information.

6.7 All personal information should be treated as sensitive and any protective or privacy markings attached to personal information must be respected. Each partner organisation should have an individual, e.g. Data Security Officer, who should be able to advise staff on protective/ privacy markings (where these are used) and their application.

6.8 Partner organisations internal Information Security policies should be made available to staff. These policies and related guidance should clearly set out how sensitive information should be stored, transmitted and eventually destroyed. They should establish that more sensitive material will require higher levels of protection and more stringent management safeguards. They should have, or should aim to develop, specific procedures for the secure disposal of personal information when it is no longer required.

6.9 The security of IT and record systems are the responsibility of individual partner organisations. These systems should aim to comply with records management standards (including ISO15489) and best practice set out by the Public Record Office of Northern Ireland (PRONI). They should also aim to comply with the International Security Standard ISO27001 and ISO27799 (Information security management in health, incorporating ISO/IEC 27002:2005 Information Technology — Security Techniques). Information Management, Information Security staff or IT Security specialists within the partner organisation should be able to advise and provide relevant guidance to staff in these areas.

6.10 Partner organisations should:

- Aim to be compliant with ISO27001 and ISO27799.
- Provide policy and procedural guidance to staff on Information Security and protective markings (where applicable).
- Produce internal policies on encryption and the use of approved devices, such as iron keys and ensure that this is rolled out across the organisation; and ensure that unapproved devices are not used by staff, as these could compromise the security of IT systems.
- Ensure the protection of IT systems from unwarranted access.
- Protect PCs and databases via the use of passwords and login IDs associated with specific staff, as well as providing support and guidance to staff on the use of and the protection of passwords and IDs.
- Designate levels of access to personal data to staff, based on the role of the member of staff and what they need to have access to, as well as internal procedures on information access security levels. Access should be provided on a 'need to know' basis.
- Make appropriate arrangements for the disposal of electronic information and information stored on back-ups, so that disposal is secure and timely.
- Maintain adequate records of any breaches and ensure that these are shared with relevant personnel and that lessons learned are recorded and necessary measures taken to ensure future breaches are prevented.

6.11 Partner organisations who share information with outside bodies must assure themselves that these bodies have adequate data security policies and procedures in place and where possible, that these are consistent with those used within partner organisations. All organisations must confirm that they comply with the appropriate security standards, based on ISO27001 and ISO27799, before information is shared.

6.12 All partner organisations must ensure that whomever they share information with can provide assurances that they comply with the DPA and that they have relevant DP policies and procedures in place, of which their staff are aware.

6.13 Partner organisations must be assured of partners arrangements for the secure management of the systems where the data is to be held, its software and its user access rights; also for the secure destruction of data that is no longer required.

6.14 Data Access Agreements should be used to provide assurances about bodies with which information is to be shared. These bodies should provide evidence of their technical security arrangements and should be able to describe the organisational security arrangements they have in place to protect shared information. Data Access Agreements should clearly require bodies to demonstrate that they have adequate Information Management and Technology (IM&T) security and confidentiality standards. They should also confirm that they either comply with, or are committed to achieving, standards set out in ISO27001 and ISO27799. The agreement may also ask them to provide copies of their IT Systems Security and Information Security policies. It should ask them to describe how security arrangements are audited and monitored.

6.15 The Data Access Agreement Framework at Appendix 2 provides guidance on the information bodies might need to seek in this area, in order to gain the proper assurance that another organisation, with which they intend to share information, has adequate IM&T safeguards and arrangements in place.

6.16 It will be the responsibility of the partner organisation that is providing the information to be shared to assure itself that the information will continue to be protected accordingly, once it is passed to the receiving body. The partner

organisation providing the information may request a visit to the partner site to monitor compliance.

Records Management

6.17 It is imperative that all partner organisations retain records of data sharing arrangements. These should include:

- Information about all requests to share information and whether or not they were approved.
- Detailed information about data that has been transferred.
- Copies of related correspondence about data sharing arrangements, e.g. notes of telephone conversations, letters and emails.
- Information about any amendments to data or deletion of data and how this has been communicated to organisations that hold copies of the same records, to ensure that all information is kept up-to-date and disposed of in line with disposal schedules.

6.18 Data inaccuracies should be reported to the relevant partner organisation. The data controller for the partner organisation must take necessary steps to ensure that the data is amended to remove inaccuracies and that other bodies, with whom the data has been shared, are informed and instructed to amend the data at their end also, within a reasonable timeframe.

Part 7

Data Sharing Legislation and Guidance

7.1 Each of the partner organisations involved with this protocol must consider the reasons for which they share personal information and whether or not their organisations, as independent statutory bodies, have the rights/powers to do so.[20] In some cases, when determining whether or not the sharing of information is lawful, partner organisations may need to seek specialist legal advice.

7.2 Sharing must be justified on the basis that the benefits, supported by meaningful safeguards, clearly outweigh the risks of negative effects and that any negative effects are kept to a minimum.[21]

Data Protection Act (DPA) 1998

7.3 The DPA is the key piece of legislation governing the protection and use of identifiable service user information (personal data).[22] The DPA clearly sets out the rights of the data subject in respect of personal data held about them by others. In general terms, the Act regulates the manner in which personal data can be collected, used and stored and so is of prime importance in the context of data sharing.

7.4 The Act places an obligation on public sector bodies that use identifiable service user information, to tell their service users how information about them may be used and who may have access to it.

7.5 Definitions which may help in understanding the language of the Act are included in the Definitions Document at Appendix 1.

[20] The Department for Constitutional Affairs (DCA) established guidance to help guide organisations in this respect, 'Public Sector Data Sharing – Guide on the Law' (November 2003).
[21] Information Commissioners Office- 'Sharing Personal Information: Our Approach' (April 2007). www.ico.gov.uk
[22] See www.dataprotection.gov.uk

7.6 There are 8 Data Protection principles set out in Schedule 1 of the Act.[23] Any processing of personal data, including sharing of data, must comply with these principles. Principles 1 and 2 are particularly relevant in relation to lawfulness of data sharing. They state that:

1. Data should be processed fairly and lawfully.
2. Data should be processed for limited, specified and lawful purposes and not further processed in any manner incompatible with those purposes.

7.7 The 1st DPA Principle also requires organisations to meet at least one of the conditions set out in Schedule 2 (for all personal data) and Schedule 3, (for sensitive personal data, which includes information relating to a person's physical or mental health), of the Act. The most relevant of these conditions in a health sector context have been highlighted by the Information Commissioner in their guidance on 'Use and Disclosure of Health Data – Guidance on the Application of the Data Protection Act 1998' (May 2002).[24] A summary of these is provided at Appendix 6.

7.8 Partner organisations must ensure that disclosures of service user identifiable information are consistent with their organisation's registration under the Act. Your organisation's Data Protection Officer, or equivalent, should be able to advise. Should you wish to use patient information for new purposes you must notify your Data Protection Officer, so that they can ensure that it is in line with the DPA and that the new purpose is added to your organisation's registration.

Code of Practice

7.9 The Code of Practice sets out the principal Laws relating to confidentiality and disclosure.[25] This includes, **The Common Law of Confidentiality, The**

[23] A list of the DPA Principles is provided as part of Appendix 4.
[24] http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/health_data_-_use_and_disclosure001.pdf
[25] Code of Practice, Appendix 2.

Human Rights Act, **DPA** and **FOIA**, as well as Northern Ireland specific law such as the Criminal Law Act (NI), Public Health Act (NI) and Mental Health (NI) Order. In line with legislation, the Code of Practice states that 'uses or disclosures' of identifiable service user information "are only justified where either:

1. service user consent has been given, or
2. there is a statutory requirement, or
3. the balance of the public and private interest favours disclosure. In such situations there must be substantial public interest favouring disclosure which outweighs both the private interests of the individual and the public interest in safeguarding confidentiality."[26]

7.10 Ethics and the Law of Confidentiality, which applies to any disclosure and use of personal information, are considered in Appendix 1 of the Code of Practice. There are 3 core ethical principles which underpin the law and which must be considered in the context of protecting service user privacy and confidentiality. These are:

1. The Individual's fundamental right to confidentiality.
2. The Individual's right to control access to and disclosure of their personal information.
3. For disclosure of confidential information to be in proportion to the need and any risks attached to it.

7.11 In relation to sharing information about children, DHSSPS are working in conjunction with other key stakeholders in developing, 'Agreed Standards and Criteria for Information Sharing for Agencies Working with Families and Children in Northern Ireland'. Once developed, this guidance will be published and shared across the HSC.

Freedom of Information (FOI)

[26] Code of Practice, Preface, Page 5, Paragraph 2.

7.12 The ICO encourages organisations to include material about information sharing in their publication scheme, as a means of helping to keep the public informed about information sharing practices. This should include providing a copy of this protocol which may be indicated, along with the Code of Practice, as standards and safeguards in place to enable sharing of information in the public interest and for the public benefit, in line with best practice and legislative requirements.

APPENDICES

Appendix 1 - Useful Definitions

Anonymised Information – Information from which no individual can be identified.

Data Controller - A person who determines the purposes for which, and the manner in which, personal information is to be processed. This may be an individual or an organisation and the processing may be carried out jointly or in common with other persons.

Data Matching - The electronic comparison of two or more sets of personal information which have been collected for separate purposes in order to identify any information that is inconsistent or overlapping. It is a form of data sharing.

Data Processor – Any person (other than an employee of the data controller), who processes the data on behalf of the data controller. Anyone responsible for the disposal of confidential waste is also included under this definition.

Data Protection Officer – Individual within an organisation who provides advice on Data Protection issues and is the point of contact for the Information Commissioner.

Data Sharing – The disclosure of data from one or more organisations to a third party organisation or organisations, or the sharing of data between different parts of an organisation. Can take the form of systematic, routine data sharing where the same data sets are shared between the same organisations for an established purpose; and exceptional, one off decisions to share data for any of a range of purposes.

Data Subject - A living individual who is the subject of the personal information (data).

Partner Organisations – The organisations who have signed up to the protocol. (See Appendix 3 for current list of organisations and their Nominated Officers.)

Personal Data - Personal data means information about a living individual who can be identified from that information or from that information and other information which is in, or likely to come into, the data controller's possession.

Privacy - The meaning of 'privacy' or 'private life' is not precisely defined for the purposes of the law. Private matters include details about a person's home, family, religion, health or sexuality.

Processing - Processing means obtaining, recording or holding the data or carrying out any operation or set of operations on data.

Sensitive Personal Data - Personal data about ethnic or racial origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health, sexual life, commission or alleged commission of offences and criminal convictions or proceedings.

Service User Identifiable Information – Information that relates to an individual service user, including their image or voice, which enables them to be uniquely identified from that information on its own or from that and / or other information available to that organisation. It includes personal data within the meaning of Section 1 of DPA and also includes information relating to the deceased.

Statutory Gateway - An express statutory power to share personal data whether permissive or mandatory.

Third Party – Any person other than the data subject, the data controller, or any data processor authorised to process data for the data controller or processor.

Appendix 2 - Data Access Agreement Framework

The following provides a framework for the information which should be captured as part of Data Access Agreements between partner organisations, when requesting to share service user information.

It sets out the key headings which should be included in any Data Access Agreement and outlines the type of information that should be provided by the requesting organisation, in order to enable the receiving organisation to make an informed decision as to whether or not the information should be shared.

Note, information under all sections, excluding section 3, should be included as part of all Data Access Agreements. Where applicants are seeking access to ***identifiable service user information*** *the* ***additional information under section 3 should be provided****.*

1 Details of the Organisation Requesting to Share Service User Identifiable Information

The name and contact details of the requesting organisation.

Contact details of the person ultimately responsible for ensuring the information is managed in accordance with data protection and data security obligations once transferred.

Any written support from the requesting organisation's Personal Data Guardian.

A description of the data subjects/ service users whom the information is about. The information being requested, including any identifier attributes (e.g. name, address, Date of Birth (D.O.B)).

Details of how the requesting organisation proposes to process the information once it is received (for example, to extract and anonymise service user information; for auditing and monitoring of service user care and treatment).

2 Principles

Assurance that the following principles for Secondary uses, from the Code of Practice, have been followed:

- Organisations seeking information other than for direct care should be seeking anonymised or pseudonymised data.

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

3 Where access to service user identifiable information is being sought the following additional information should be provided

a Justification of Purpose

A comprehensive description of all purposes of the work, for which the service user identifiable information is being sought. Reasons/ benefits of the work. An explanation of why all of the elements of the data requested are required (e.g. why names, postcodes and HSC numbers are needed).

b Consent Issues

An explanation of why it is impractical for either the requesting organisation, or the organisation that owns the information, to obtain consent from the service users. Include evidence to support assertions made.

c Anonymisation Issues

Justification for the use of the service user identifiable data, including details of:

- Consequences if the work/activity, which requires the service user identifiable data, does not go ahead.
- Steps which may be taken to move towards developing anonymised or coded data in the future to support the work/activity.

4 Data Protection Issues

Information about how the requesting organisation meets the requirements of the Data Protection Act, (especially the 8 DPA principles), and other legislation.

Details about confidentiality including confidentiality policies.

5 Security Issues

Steps taken to limit the use/processing of service user identifiable information and access to this information.

Evidence of adequate IM&T security standards including physical security, system information security, system auditing and monitoring arrangements, data retention and destruction, (including justification if information needs to be kept for longer than 12 months and notification of how and when information has been destroyed via use of Data Destruction Notification Forms).

Evidence that the organisation is registered on the ICO's DPA Register of Data Controllers and that the purposes listed under their registration adequately cover the purposes listed as part of this agreement.

6 Terms and conditions

Terms and conditions of the agreement, which may include:

- That the data must not be shared beyond the requesting organisation and the scope of the agreement.

- That the supplying organisation has the right to inspect the premises and processes of the requesting organisation to ensure that they meet the standards set out in the agreement. That they also have the right to withdraw access if they find the requesting organisation does not meet the standards, or has breached the agreement.

- That any loss, theft or corruption of the shared data by the requesting organisation must be immediately reported to the authorising officer of the supplying organisation.

7 Authorising Officer Sign Off

The agreement should be signed and dated by the Information Custodian of the requesting organisation and the Personal Data Guardian, or other appropriate approved officer within the owning organisation, who has approved the agreement.

Appendix 3 - Partner Organisations & Nominated Officers(s)

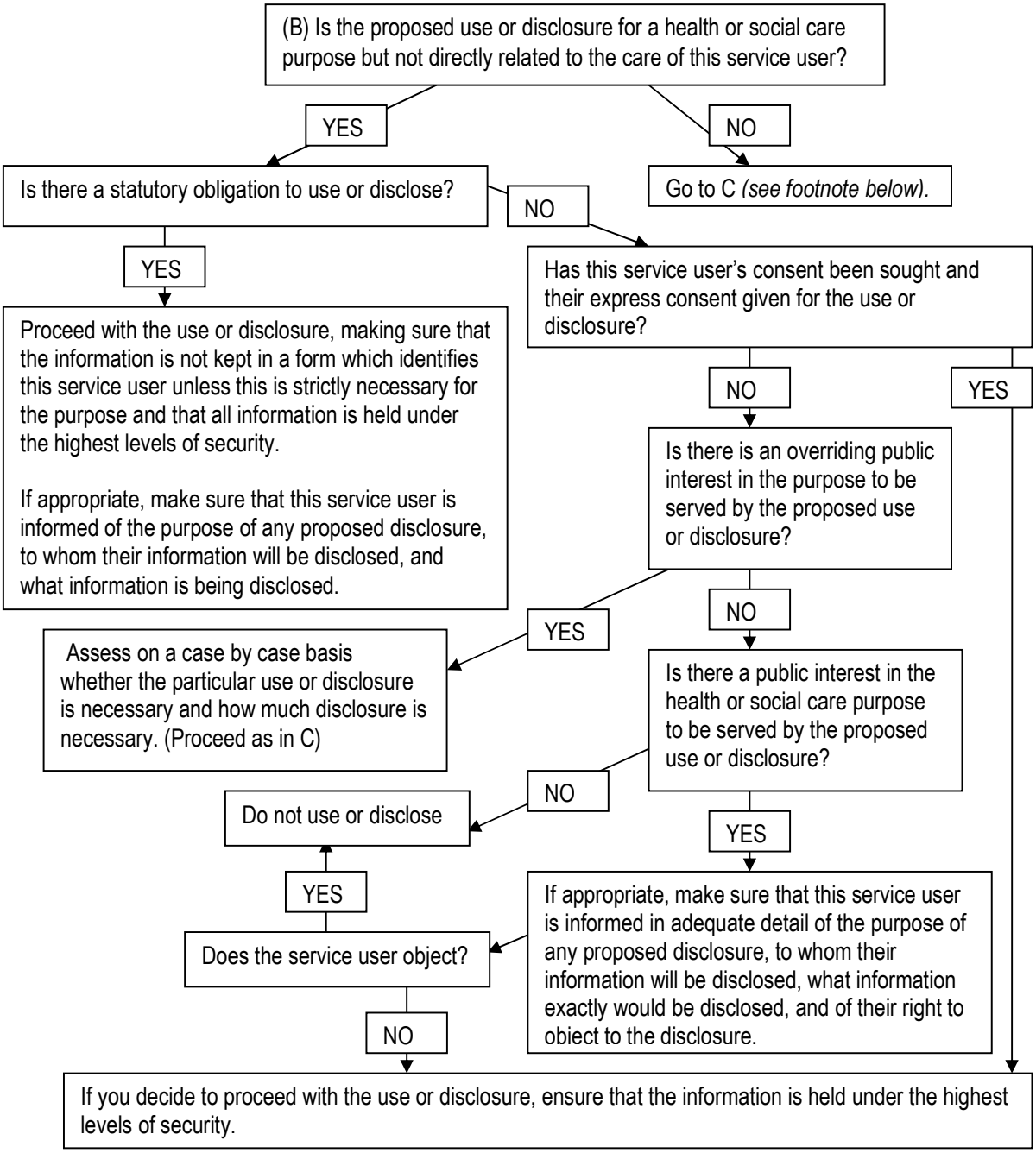
Organisation	Nominated Officer(s)/ PDGs
Department of Health, Social Services & Public Safety (DHSSPS)	Dr Paddy Woods
Health & Social Care Board	Bernard Mitchell
Belfast Health & Social Care Trust	Bernie McNally Sharon Kelly Tony Stevens
Northern Health & Social Care Trust	Peter Flanagan
South Eastern Health & Social Care Trust	Charlie Martyn Ian Sutherland
Southern Health & Social Care Trust	Brian Dornan Patrick Loughran
Western Health & Social Care Trust	John Doherty Dr Anne Kilgallen
Business Services Organisation (BSO)	Hugh McPoland
NI Ambulance Service Health & Social Care Trust	Dr David McManus
NI Blood Transfusion Service (NIBTS)	Geoff Geddis
NI Guardian Ad Litem Agency (NIGALA)	Lily Barr
NI Medical & Dental Training Agency (NIMDTA)	Dr Terry McMurray
Northern Ireland Practice & Education Council for Nursing and Midwifery (NIPEC)	Edmund Thom
NI Fire & Rescue Service (NIFRS)	Doros Michail
Health & Social Care Regulation and Quality Improvement Authority (RQIA)	Glenn Houston
NI Social Care Council (NISCC)	Mark Bradley
Patient and Client Council (PCC)	Sean Brown
Public Health Agency	Ed McClean

Appendix 4 - Principles Governing Information Sharing[27]

Code of Practice 8 Good Practice Principles[28]	DPA Principles	PDG Principles[29]
1. 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 the users may have. **2.** Where an organisation has a direct relationship with a service user then it should be aiming to implement procedures for obtaining the express consent of the service user. **3.** Where consent is being sought this should be by health and social care staff who have a direct relationship with the individual service user. **4.** 'Third Party' organisations seeking information other than for direct care should be seeking anonymised or pseudonymised data. **5.** Any proposed use must be of clear general good or of benefit to service users. **6.** Organisations should not collect secondary data on service users who opt out by specifically refusing consent. **7.** 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. **8.** To assist the process of pseudonymisation the Health and Care Number should be used wherever possible.	**1.** Data should be processed fairly and lawfully. **2.** Data should be processed for limited, specified and lawful purposes and not further processed in any manner incompatible with those purposes. **3.** Processing should be adequate, relevant and not excessive. **4.** Data must be accurate and kept up to date. **5.** Data must not be kept longer than necessary. **6.** Data must be processed in line with the data subject's rights (including confidentiality rights and rights under article 8 of the Human Rights Act). **7.** Data must be kept secure and protected against unauthorised access. **8.** Data should not be transferred to other countries without adequate protection.	**1.** Justify the purpose(s) for using confidential information. **2.** Only use it when absolutely necessary. **3.** Use the minimum that is required. **4.** Access should be on a strict need-to-know basis. **5.** Everyone must understand his or her responsibilities. **6.** Understand and comply with the law.

[27] These principles must be followed by health and social care organisations when considering use and disclosure of service user information.
[28] Code of Practice, paragraph 3.17.
[29] PDG Principles are adopted from the Caldicott Principles established in England and Wales.

Appendix 5 - Code of Practice Secondary Uses/ Purposes Flow Diagram[30]



[30] This flow diagram outlines the key considerations in making good decisions about the use and disclosure of service user identifiable information for secondary uses (see para 3.28 – 3.30 of the Code of Practice). It covers the use of this information for "purposes of health and social care not directly related to the care of that service user". (para 3.29(B) of the Code of Practice). **Note reference 'Go to C'** refers to a further flowchart provided in the Code of Practice, which covers 'disclosure for other purposes' (provided on page 23, Code of Practice).

Appendix 6 - Summary of DPA Schedule 2 and Schedule 3 Conditions Relevant in a Health Sector Context[31]

Schedule 2:

- Processing with the consent of the data subject;
- Processing necessary to protect the vital interests of the data subject;
- Processing necessary for the exercise of functions of a public nature exercised in the public interest;
- 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 processing is prejudicial to the rights and freedoms or legitimate interests of the data subject.

Schedule 3:

- Processing with 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, obtaining legal advice, or is otherwise necessary for the purposes of establishing, exercising or defending legal rights;
- The processing is necessary for medical purposes and is undertaken by a health professional or a person owing a duty of confidentiality equivalent to that owed by a health professional.

Further Schedule 3 conditions added under the Data Protection (Processing of Sensitive Personal Data) Order 2000:

- Processing of medical data or data relating to ethnic origin for monitoring purposes;
- Processing in the substantial public interest, necessary for the purpose of research whose object is not to support decisions with respect to any particular data subject otherwise than with the explicit consent of the data subject and which is unlikely to cause substantial damage or substantial distress to the data subject or any other person.

[31] Taken from Information Commissioner Guidance 'Use and Disclosure of Health Data – Guidance on the Application of the Data Protection Act 1998' (May 2002), pages 3-4.

Appendix 7 - Further Information & Guidance

'Data Sharing Code of Practice', available from, www.ico.gov.uk

'Framework Code of Practice for Sharing Personal Information', available from, www.ico.gov.uk

'Guide to Data Protection', available from, www.ico.gov.uk

'Privacy Impact Assessment (PIA) Handbook', available from, www.ico.gov.uk

'Privacy Notices Code of Practice', available from, www.ico.gov.uk

'Sharing Personal Information: ICO Approach', available from, www.ico.gov.uk

'Use and Disclosure of Health Data – Guidance on the Application of the Data Protection Act 1998', available from, http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/health_data_-_use_and_disclosure001.pdf

'Public Sector Data Sharing – Guide on the Law', available from, http://www.justice.gov.uk/about/docs/data_sharing_legal_guidance.pdf

Data Sharing Management Guidance from the Department of Constitutional Affairs (DCA), available from, www.foi.gov.uk/sharing/toolkit/manguide.htm

'A Toolkit for Data Sharing', available from, http://www.foi.gov.uk/sharing/toolkit/index.htm

NHS Leeds 'Information Sharing Protocol', 'Operational Procedures' and 'Staff Guidance', available from, http://www.leedspct.nhs.uk/about/?pagepath=About%20Us/Information%20Sharing/Protocol