



# Data Sharing across the Highland Data Sharing Partnership

## **Procedures for Practitioners**

Version 1.9

<b>Policy Reference:</b> ISP Information Sharing Procedures – Version v1.9	
<b>Prepared by:</b> ISP review group of DSP	<b>Date of Issue:</b> May 2008
<b>Lead Reviewer:</b> Director of Community Care, NHS Highland	<b>Date of Review:</b> May 2010

<b>Distribution</b> <ul style="list-style-type: none"> <li>• NHS Highland – Jan Baird</li> <li>• Northern Constabulary – Ian Williams</li> <li>• Highland Council – Miles Watters</li> <li>• Argyll and Bute Council – Gavin Boyd</li> <li>• Strathclyde Police – Raymond Park</li> </ul>			
<b>Method</b>			
CD Rom	E-mail X ✓	Paper X	



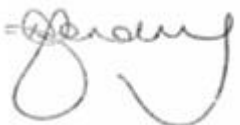
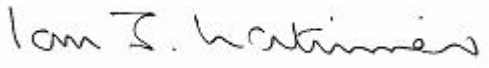
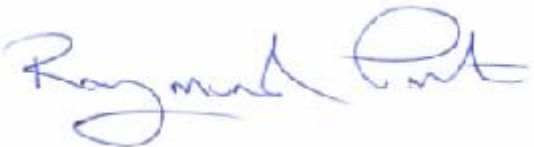
<b>Warning – Document uncontrolled when printed</b>	

## Forward

The sharing of personal information across agencies is an issue which staff often find confusing and difficult. The Highland Data Sharing Partnership, established in 2007, prioritised the development of procedures which would support practitioners across the services. These procedures have been developed by a core group drawn from all public sector partners and have been circulated across agencies for wider consultation.

We understand the issues for our staff and the need for clarity and consistency in decision making. These procedures will benefit the people of Highland and their families by enabling effective integrated working where appropriate information can be shared, relevant confidentiality protected and personal information is safely managed.

We will ensure these procedures and the Information Sharing Policy which support them will be available to all staff. The Data Sharing Partnership will continue to monitor the procedures ensuring any necessary updates as a result of legislative change are communicated across all staff groups. The Data Sharing Partnership will also monitor the effectiveness of these procedures to ensure appropriate support to staff and continued development of effective integrated working.

Dr Roger Gibbins, Chief Executive, NHS Highland	
Mr Alistair Dodds, Chief Executive, The Highland Council	
Mr Douglas Hendry, Director of Community Services, Argyll & Bute Council	
Mr Ian Latimer, QPM, MA, Chief Constable, Northern Constabulary	
Superintendent Raymond Park, Strathclyde Police	

# CONTENTS

## 1. Overview and Purpose

- 1.1 Introduction
- 1.2 Purpose
- 1.3 Definitions

## 2. Legislation Governing Data Sharing

- 2.1 Introduction
- 2.2 The Data Protection Act 1998
- 2.3 Human Rights Act 1998
- 2.4 The Children (Scotland) Act 1995
- 2.5 Common Law and Statutory Obligations of Confidence
- 2.6 Freedom of Information (Scotland) Act 2002
- 2.7 Adults with Incapacity (Scotland) Act 2000
- 2.8 Other Relevant Legislation
- 2.9 Summary
- 2.10 Legislation flowchart

## 3. Consent

- 3.1 Introduction
- 3.2 What is Consent?
- 3.3 Who can give Consent?
- 3.4 How to Obtain and Record Consent
- 3.5 Sharing Data about an unborn Child
- 3.6 If Consent is Refused or Withdrawn
- 3.7 Circumstances in which Consent Should Not be Sought
- 3.8 Sharing Data without Consent
- 3.9 Summary
- 3.10 Consent Flowchart

## 4. Methods of sharing data between agencies

- 4.1 Introduction
- 4.2 Verbal Communication
- 4.3 Written Communication
- 4.4 E-mail Communication
- 4.5 Fax Transfer
- 4.6 The Government Protective Marking Scheme
- 4.7 NHS Confidential Information
- 4.8 How to Request Data from another Agency

## 5. Resolving Disputes

- 5.1 Introduction
- 5.2 Disputes between Practitioners
- 5.3 Complaints from Members of the Public

## 6. Summary of Key Points

### Appendices

- Appendix A The Six Caldicott Principles
- Appendix B Sample Consent Form
- Appendix C Sample Leaflets
- Appendix D References

# 1. Overview and Purpose

## 1.1 Introduction

Effective integrated working requires timely, proportionate and appropriate data sharing. These procedures provide practitioners with guidance to assist them to do this. These procedures are applicable to all practitioners involved in sharing data with another agency within the Highland Data Sharing Partnership area. These procedures apply equally to those practitioners who are asked to share data and to those who have data they feel should be shared.

## 1.2 Purpose

The purpose of these Procedures is;

- To describe briefly relevant legislation and to explain how this provides a framework for sharing data between agencies,
- To describe when and how consent for data sharing should be sought,
- To describe appropriate methods for data sharing between agencies, and
- To describe how to resolve disputes over data sharing between agencies.

## 1.3 Definitions

Within these procedures the following definitions are used:

*Data Controller* means a person (normally at corporate or executive level) who determines on behalf of an organisation the purposes for which, and the manner in which, data is processed and shared.

*Data Processing* means obtaining, recording or holding data or carrying out any operation or set of operations on the data, including;

- organisation, adaptation or alteration of the data,
- retrieval, consultation or use of the data,
- disclosure of the data, or
- alignment, combination, blocking, erasure or destruction of the data;

*Data Protection Officer* means the position within an agency that has been designated to respond to subject access requests and/or to provide guidance on all aspects of the Data Protection Act. In some agencies this position may be designated by another title.

*Data Sharing* means the sharing of personal data and/or sensitive personal data between agencies within the Highland Data Sharing Partnership.

*Data Subject* means the person user to whom data refers.

*European Economic Area (EEA)* means the EU Member states and Iceland, Lichtenstein and Norway.

*Highland Data Sharing Partnership* means the partnership comprising Highland Council, Argyll and Bute Council, Northern Constabulary, Strathclyde Police and NHS Highland.

*Information Officer* means the position within an agency that has been designated to respond to freedom of information and environmental requests. In some agencies this position may be designated by another title.

*Personal Data* means data relating to a living person which includes the identity of the data subject or from which the identity of the data subject can be inferred.

*Public Authority* means;

- Central Government Departments and Agencies,
- Local Government,
- Police,
- NHS,
- State schools, colleges and universities, and
- Publicly owned companies.

*Sensitive Personal Data* means data relating to a living person from which the identity of that person can be established or inferred AND includes one or more of the following;

- The racial or ethnic origin of the subject,
- The political opinions of the subject,
- The religious beliefs or other beliefs of a similar nature of the subject,
- Whether the subject is a member of a Trade Union,
- The physical or mental health or condition of the subject,
- The sexual life of the subject, or
- Information relating to the commission or alleged commission of any offence by the subject.

## 2. Legislation

### 2.1 Introduction

It is a common misconception that legislation prevents data sharing. It does not. The relevant pieces of legislation require that an assessment is made of whether the potential benefits of a specific instance of data sharing outweigh the potential risks. Some legislation follows a prescriptive approach, detailing criteria that should be used to make this assessment. Other legislation takes a broader approach, leaving the individual practitioner to make their own assessment. The purpose of both types of legislation is not to prevent data sharing but to ensure that sharing is proportionate and appropriate.

In most cases, using legislation to assess whether to share data will only be relevant where explicit consent for sharing has not been given by a data subject. Where consent has been given, and there is a need-to-know, data may be shared. Where consent has not been given, but there is a need-to-know, legislation assists the practitioner to decide whether sharing should take place. Legislation supports the commonsense approach to making this decision – if data is to be shared to **prevent harm**, to **prevent or detect crime** or to **improve the wellbeing of individuals or groups** or for **public protection** and if the information to be shared is **relevant and proportionate**, then data should be shared. In addition, if a child is considered to be at risk of harm, relevant data must always be shared.

Several pieces of legislation apply to data sharing in the UK. The specific focus of each piece of legislation is different, though in general the requirements of all of them are complimentary. This section provides an overview of the requirements of each relevant piece of legislation and guides the reader to sources of further information.

In addition to the legislation described here, sharing data between the NHS and other agencies is also governed by the Caldicott Guardians. These guardians were appointed in NHS areas following a report by the Caldicott Committee in 1997. The committee also established six principles for the safe sharing of sensitive personal data with agencies outside the NHS (these principles are detailed in Appendix A to this document). The principles are broadly aligned with the requirements of the Data Protection Act. The Caldicott Guardians are responsible for ensuring that NHS Practitioners comply with the six principles. These principles only apply to the NHS. However other agencies should be aware that in addition to legislation and codes of practice, these guidelines are used by NHS practitioners when deciding whether to share data.

## 2.2 The Data Protection Act 1998

### Introduction

The *Data Protection Act 1998* (DPA) was passed into UK law in 1998 and came into force in 2001. This is the main piece of legislation governing the processing and sharing of data in the UK. The DPA places obligations on those who process and share data and gives rights to those who are the subject of that data. Compliance with the DPA is overseen in the UK by the Information Commissioner's Office (ICO).

The DPA requires any agency processing personal data to notify the ICO that they are doing so. All agencies within the Highland Data Sharing Partnership have notified the ICO that they are processing personal data.

The purpose of the DPA is not to prevent data sharing, but to ensure that a balance is struck between the right to privacy and the need for public authorities to share data to protect individuals and the public interest. The DPA applies to some paper records as well as computer records.

The DPA provides a framework to assist practitioners to assess whether the **benefits** of a specific instance of data sharing for society or for individuals outweigh the **risks** to personal privacy. The DPA does this by providing eight data protection principles (Schedule 1) that set out the way in which all data is to be processed. In addition the DPA provides conditions that must be used to judge whether *personal data* may be shared (Schedule 2) and additional conditions that must be used to judge whether *sensitive personal data* may be shared (Schedule 3). By ensuring that these principles and conditions are met it will be possible to demonstrate that data is processed appropriately and that the benefits of a particular instance of data sharing clearly outweigh the risks.

### The Eight Data Protection Principles

Schedule 1 of the DPA sets out eight data protection principles. These define how data must be processed. They state that data must be:

1. fairly and lawfully processed,
2. processed for limited purposes,
3. adequate, relevant and not excessive,
4. accurate and up to date,
5. not kept longer than necessary,
6. processed in accordance with the individual's rights,
7. secure, and

8. not transferred to countries outside European Economic Area unless the country to which the data is to be transferred has adequate protection for the individual.

The Data Controller must satisfy themselves that any data that they have responsibility for is processed in accordance with these principles.

### **The Need to Know**

The DPA requires that the first step when considering whether to share data is to ensure that the person requesting the data has a legitimate need-to-know. If necessary, the practitioner should contact this person to clarify and expand upon the reasons for data sharing. Only when the practitioner is satisfied that a legitimate need-to-know exists should data sharing be considered.

As a simple rule-of-thumb, to demonstrate a need-to-know a person must be able to show that the public agency function they are required to perform cannot be effectively completed without the information requested.

### **Scope of the DPA**

When the practitioner has established that there is a legitimate need-to-know, the next thing to consider is whether the data to be shared comes within the scope of the DPA. The DPA relates only to information on identified or identifiable living persons. So for example, if the data subject is dead, or if anonymised data is to be shared, the information is not subject to the DPA. It should also be noted that mere reference to a person's name where no other personal information is given or can be inferred (for example, a note of a person's attendance in the minutes of a meeting or inclusion of a name in a distribution list) does not come within the scope of the DPA.

### **DPA Conditions for data sharing – Schedule 2**

If the data to be shared comes within the scope of the DPA, the reasons for sharing must meet at least one of the conditions defined in Schedule 2 of the DPA. These are:

1. The data subject has given consent for data sharing.
2. Sharing is necessary-
  - a. for the performance of a contract to which the data subject is a party, or
  - b. at the request of the data subject with a view to entering into a contract.
3. The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.
4. The processing is necessary in order to protect the vital interests of the data subject.
5. The processing is necessary-

- a. for the administration of justice,
  - b. for the exercise of any functions conferred on any person by or under any enactment,
  - c. for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or
  - d. for the exercise of any other functions of a public nature exercised in the public interest by any person.
6. The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

It will be seen that these are very broad conditions. Most of the data shared within the agencies of the Highland Data Sharing Partnership will be covered by conditions 1, 3, 4, 5a, 5d or 6.

If the data to be shared is personal data, and the reasons for sharing satisfy at least one of the above conditions, the data may be shared.

### **DPA Conditions for data sharing – Schedule 3**

If the data to be shared is sensitive personal data, the reasons for sharing must satisfy one of the conditions above AND one of the conditions from Schedule 3 of the DPA. These are:

1. The data subject has given explicit consent for data sharing.
2. The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.
3. The processing is necessary-
  - a. in order to protect the vital interests of the data subject or another person, in a case where-
    - i. consent cannot be given by or on behalf of the data subject, or
    - ii. the data controller cannot reasonably be expected to obtain the consent of the data subject, or
  - b. in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.
4. The processing-
  - a. is carried out in the course of its legitimate activities by any body or association which-
    - i. is not established or conducted for profit, and
    - ii. exists for political, philosophical, religious or trade-union purposes,

- b. is carried out with appropriate safeguards for the rights and freedoms of data subjects,
  - c. relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes, and
  - d. does not involve disclosure of the personal data to a third party without the consent of the data subject.
5. The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.
6. The processing-
  - a. is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),
  - b. is necessary for the purpose of obtaining legal advice, or
  - c. is otherwise necessary for the purposes of establishing, exercising or defending legal rights.
7. The processing is necessary-
  - a. for the administration of justice,
  - b. for the exercise of any functions conferred on any person by or under an enactment, or
  - c. for the exercise of any functions of the Crown, a Minister of the Crown or a government department.
8. The processing is necessary for medical purposes and is undertaken by-
  - a. a health professional, or
  - b. a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.
9. The processing-
  - a. is of sensitive personal data consisting of information as to racial or ethnic origin,
  - b. is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and
  - c. is carried out with appropriate safeguards for the rights and freedoms of data subjects.
10. The personal data are processed in circumstances specified in an order made by the Secretary of State for the purposes of this paragraph (for example, a Sensitive Data Order, SI 417, covers the Police in the exercise of their common-law powers).

If the data to be shared is sensitive personal data, and the reasons for sharing satisfy at least one of the conditions from Schedule 2 AND at least one of the conditions from Schedule 3, the data may be shared.

It should be noted that if the data subject has given explicit consent for data sharing, this satisfies the requirements of Schedule 2 and 3 of the DPA. Consent is discussed further in Section 3 of this document.

### **Sharing Information to Detect and Prevent Crime**

The DPA includes an exemption to allow the sharing of data to detect or prevent crime. Data may be shared to detect or prevent crime without meeting the conditions of Schedule 2 or 3 of the DPA (DPA Section 29, *Crime and Taxation*) though there are limits on what may be released.

The Police are most likely to ask for the sharing of data under this exemption, though other organisations may also do so because they have a crime prevention or law enforcement function. This might include for example, agencies involved in the investigation of tax or benefit fraud.

This exemption does not cover the sharing of all data in all circumstances. It only allows the sharing of data for the stated purposes and only if not releasing it would interfere with the prevention or detection of crime.

For every request for data received under this exemption (and about each separate individual), the following questions should be asked;

- Is the person requesting the data who they say they are? (Particular care should be taken if the request is received over the telephone.)
- Is the person asking for this data doing so to prevent or detect a crime or catch or prosecute an offender?
- If this data is not shared, will this impede any attempt to prevent crime or catch a suspect?
- If this data is shared, what is the minimum that can be shared to achieve the stated purpose?
- What else (if anything) needs to be known to be sure that the exemption applies?

There may also be times when personal information may be shared relating to more than one person who is not named but who may fit a particular description. For example: the Police may not have the name of a suspect, but they believe the person is known to a particular agency and have a description. In this situation, it may be reasonable to release the personal information of all the persons known to an agency who match that particular description. However, the Data Controller would need to be satisfied that the police have narrowed the range of possible suspects as much as they reasonably can.

## Other Exemptions

Part IV of the Data Protection Act provides details of other circumstances when data may be shared without meeting the conditions of Schedules 2 and 3 of the DPA. These include the sharing of data to safeguard national security, for regulatory activities and in a number of specified circumstances as ordered by the Secretary of State.

It is the responsibility of the Data Controller to satisfy themselves that any request for data sharing made under these exemptions is fair, reasonable and proportionate.

## Subject Access Requests

Individuals have a right under the DPA to make a request in writing for a copy of the information held about them by public authorities on computer and in some manual filing systems. This is called a *subject access request*. A reply to a subject access request must be provided by the public authority within 40 days.

If you receive a subject access request, you should pass it to the appropriate person in your agency, for example, the Data Protection Officer. If a subject access request is received regarding information relating to another agency, authorisation must be sought from the originating agency to release that information.

## DPA Summary

- Personal data must be processed in accordance with the eight principles of the DPA (detailed in Schedule 1)
- Personal data must be shared ONLY if there is a need-to-know
- If personal data, at least one of the conditions from Schedule 2 must be met in order to share
- If sensitive personal data, at least one of the conditions from Schedule 2 AND one of the conditions from Schedule 3 must be met in order to share
- Data may be shared without meeting the conditions of Schedule 2 and 3 if the purpose of sharing is covered by an exemption, such as to detect or prevent crime
- Individuals have a right to request a copy of information held about them – these are known as *subject access requests*

Further information on the Data Protection Act may be found at the following website:

[http://www.ico.gov.uk/for\\_organisations/data\\_protection\\_guide.aspx](http://www.ico.gov.uk/for_organisations/data_protection_guide.aspx)

## 2.3 The Human Rights Act 1998

### Introduction

The *Human Rights Act 1998* (HRA) came into force in the UK on 2<sup>nd</sup> October 2000. This Act enacts into UK law the European Convention on Human Rights. The Act defines a number of fundamental rights and freedoms that apply to all citizens of the European Economic Area. The HRA is a type of higher law, affecting all other laws. An Act of the Scottish Parliament may not include provisions which are incompatible with rights defined within the Act.

The Human Rights Act contains two key principles at its core:

- Proportionality
- The Rule of Law

*Proportionality* means that rights guaranteed under the Act must be supported in a way that is proportional to the needs of society. For example, limiting some rights of an individual may be necessary to support the rights and freedoms of others.

The *Rule of Law* means that certain rights can be subject to a limited amount of interference by public authorities in order to benefit society as a whole rather than just the individual.

In data sharing terms this can mean that one right may have to be balanced against another. For example, one person's right to respect for privacy may have to be balanced against another's right to protection against being treated in a way that is degrading or inhuman. To facilitate this balancing of one right against another, the rights given under the act are categorised into a hierarchy of three distinct types. These are:

*Absolute rights* such as the right to protection from torture, inhuman and degrading treatment, the prohibition on slavery and protection from retrospective criminal charges. These rights may not be interfered with in any circumstances and will take precedence over other rights.

*Limited rights* such as the right to liberty which are limited under circumstances defined in the Act.

*Qualified rights* such as the right to respect for privacy and family life, religious belief and freedom of expression. Interference with these rights is permissible in certain circumstances.

### Article 8

Article 8 of the Convention is of particular relevance to data sharing. Article 8 states that:

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

*8.2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.'*

Article 8 covers the sharing of personal data as well as issues such as telephone tapping, parental access and custody of children.

So, Article 8 is a *qualified right* that allows a public authority to interfere where that interference is:

- in accordance with law;
- necessary in a democratic society; and
- in pursuit of a legitimate aim.

The HRA does not pre-empt the requirements of other areas of law (although there is some overlap). For example, the requirements of the DPA must also be satisfied. However, in most cases if the conditions described in Schedules 2 and 3 of the DPA are met when data is shared, the requirements of the HRA will also be met.

Further information on the Human Rights Act can be found at the following website:

<http://www.scotland.gov.uk/Publications/2004/10/20158/45773>

## **HRA Summary**

- Based on *proportionality* and *rule of law*
- Three types of right:
  - Absolute
  - Limited
  - Qualified
- May be necessary to balance one right against another when deciding whether to share – absolute rights take precedence

## **2.4 The Children (Scotland) Act 1995**

The Children (Scotland) Act 1995 defines parental responsibilities and rights in relation to children. It also sets out the duties and powers available to public authorities to support children and their families and to intervene when the child's welfare requires it.

The Act incorporates provisions which conform to, and in some cases surpass, commitments under the UN Convention on the Rights of the Child. It also takes account of obligations under the European Convention on Human Rights. Two of the main themes running through the Act are relevant to data sharing. These are:

- the welfare of the child is the paramount consideration, and
- the child's views should be taken into account where major decisions are to be made about his or her future.

This does not conflict with the requirements of the Data Protection Act or the Human Rights Act. It simply means that whenever a decision is made about whether or not to share data when a child is involved, the welfare of the child will be the main consideration. To ensure this is considered the practitioner must ask:

- Is data sharing in the best interests of the child?, and
- Will the risk to the child be increased by not sharing?

In addition, wherever possible, the child should be consulted and their views should be taken into consideration when deciding whether to share data.

Further information on the Children (Scotland) Act can be found at the following website:

[http://www.opsi.gov.uk/acts/acts1995/Ukpga\\_19950036\\_en\\_1.htm](http://www.opsi.gov.uk/acts/acts1995/Ukpga_19950036_en_1.htm)

## **2.5 Common Law and Statutory Obligations of Responsibility**

Under Scottish law, public authorities have a common law duty of confidentiality towards the information they hold on individuals. However, confidentiality is not an absolute right. Just as described for other legislation, acting in the public interest is a defence to an accusation of breach of confidence, provided it can be demonstrated that the information shared is necessary and proportionate.

Unfortunately the law of Scotland does not set out in detail how the need for confidentiality should be balanced against the need to share data to protect the public interest. In general, if it can be shown that the requirements of the Data Protection Act and Human Rights Act have

been taken into consideration when deciding whether it is appropriate to share data, the requirements of Scottish common law and statutory obligations will also be met.

Further information on this topic can be found at the following website:

<http://www.scotland.gov.uk/Publications/2004/10/20158/45774>

## **2.6 Freedom of Information (Scotland) Act 2002**

The Freedom of Information (Scotland) Act 2002 (FOI(S)A) came into force at the beginning of 2005. This Act gives the public a right of access to information held by public authorities in Scotland. They can request access to this information by letter or e-mail. In addition, public authorities are obliged to make information available through a publication scheme. The Act is fully retrospective and applies to all information, not just information created or filed since the Act came into force. The Act requires public authorities to respond to FOI(S)A requests.

When responding to FOI(S)A requests, there are procedural requirements set out in the Act which a public authority must follow. There are also valid reasons for withholding information, which are known as exemptions from the right to know.

Practitioners must be aware that any data they record may be retained under the records management policy of their agency and may be the subject of an information access request under the FOI(S)A. If a practitioner receives an FOI(S)A request, they should refer this to the Information Officer in their agency.

If an FOI(S)A request is received for information received from another agency, the request will be referred back to the originating agency.

Further information on the Freedom of Information (Scotland) Act may be found at the following website:

<http://www.itspublicknowledge.info/Law/FOISA/FOISA.asp>

## **2.7 Adults with Incapacity (Scotland) Act 2000**

The Adults with Incapacity (Scotland) Act 2000 was one of the first pieces of social legislation passed by the Scottish Parliament.

The Act provides a range of options to help those who are or may become incapable of looking after their own affairs. It also describes the arrangements for making decisions on behalf of adults (people aged 16 or over) who lack the capacity to take some or all decisions for themselves. This generally involves appointing a person as guardian or who has power of

attorney for the data subject. This person can also give consent for data sharing on behalf of a data subject.

Under this Act, no one can provide consent on behalf of an adult in the absence of a court order or other legal authority. In cases where a data subject is unable to make their own decisions, the practitioner must be satisfied that someone has the legal authority to give consent on their behalf. Generally, this means a person who has been appointed as a guardian or who has power of attorney under an Order based on this Act or other legal authority.

For more information on the Adults with Incapacity (Scotland) Act 2000, please visit the following website;

<http://www.opsi.gov.uk/legislation/scotland/acts2000/20000004.htm>

## **2.8 Other Relevant Legislation**

### **Environmental Information Scotland Regulations 2004**

The Environmental Information Regulations allow the public to request environmental information from public authorities.

The information covered is divided into the following six areas:

- The state of the elements of the environment, such as air, water, soil, land, fauna,
- Emissions and discharges, noise, energy, radiation, waste,
- Measures and activities such as policies, plans, and agreements affecting or likely to affect the state of the environment,
- Reports, cost-benefit and economic analyses,
- The state of human health and safety, contamination of the food chain, and
- Cultural sites and built structures.

If a public authority receives a request from an individual for environmental information on any of the areas mentioned above, they are legally obliged to provide it, usually within 20 working days. There are a number of exceptions to this rule, and these must be explained if a request is refused.

If a practitioner receives a request for environmental information, they should refer this to the Information Officer in their agency.

Further information on this topic may be found at this website:

<http://www.itspublicknowledge.info/Law/EIRs/EIRs.asp>

## Information Sharing Protocols

Several other documents provide guidance to practitioners on specific instances of data sharing (for example, data sharing in relation to the control of anti-social behaviour, data sharing in relation to child protection, etc.). These documents are known as protocols and are listed in the Highland Data Sharing Policy. Practitioners should make reference to these protocols when undertaking the specific types of data sharing identified in these documents.

## 2.9 Summary

None of the legislation described here seeks to prevent data sharing. Instead, legislation provides a framework within which practitioners can be assured that data sharing is done securely, proportionately and appropriately. Legislation is based upon common-sense principles that require the risks and benefits of data sharing to be balanced against the benefits. This is not something new. Practitioners are already doing this as part of their day-to-day activities. Legislation simply seeks to formalise and standardise this process.

The legislative criteria for assessing whether data should be shared without consent are provided in this section, but the main circumstances where data will be shared without consent include:

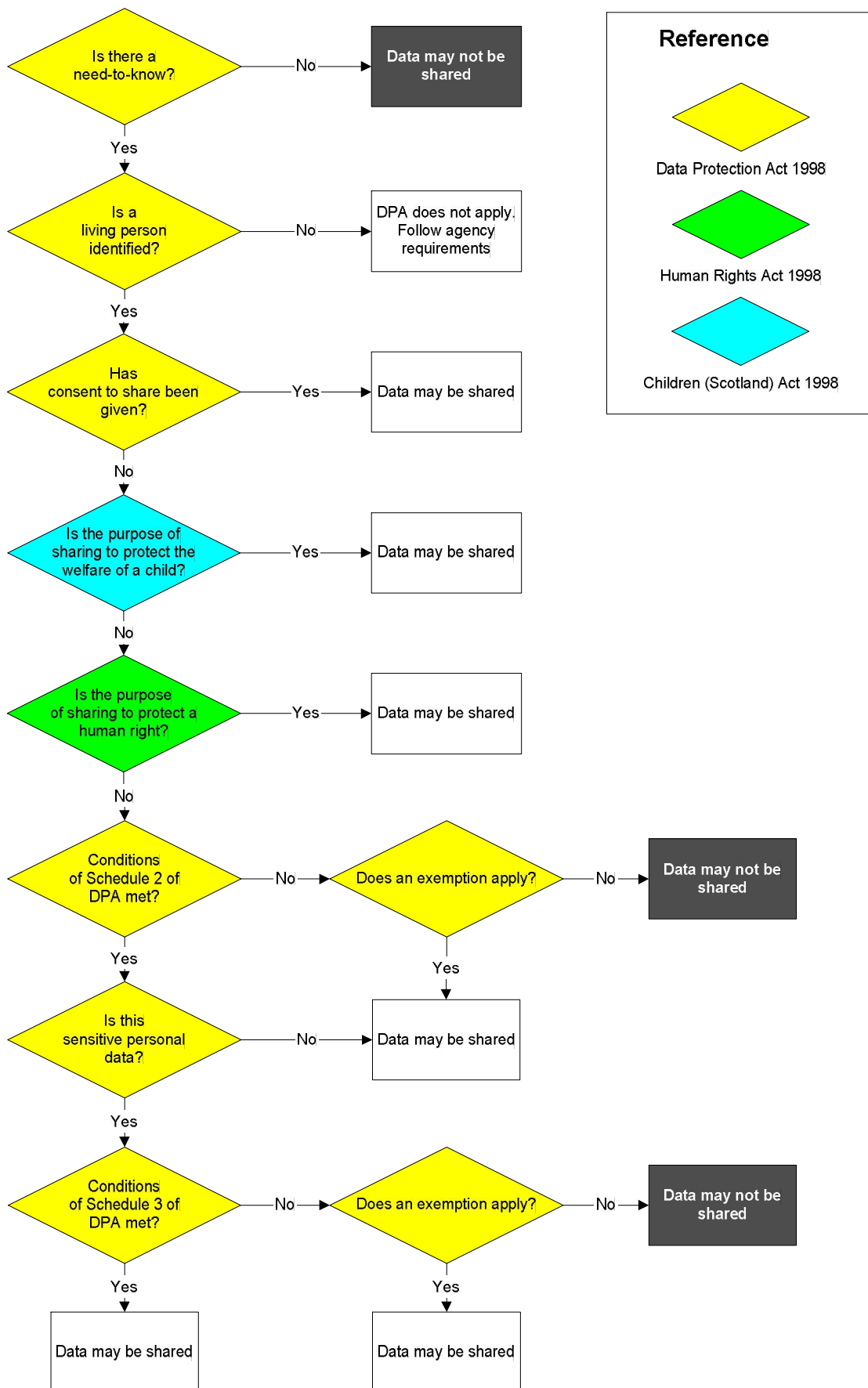
- Where failure to share data may constitute a serious breach of the duty of care,
- When a child is believed to have been abused or is at risk of significant harm,
- When there is evidence of serious public harm or risk of significant harm to others,
- Where there is evidence of a serious risk to an individual,
- For the prevention and detection of crime,
- When instructed to do so by the court, or
- Where there is a statutory requirement, e.g. where information is required by a Children's Reporter as part of their investigation of a child referred to them.

Where data is shared without consent, it is important that the data shared, with whom it is shared and the reasons for sharing are recorded. Where it will not cause harm, the data subject should also be provided with this information when data is shared about them without their consent.

Where the data subject has provided consent, and the data controller is satisfied that there is a genuine need to know, data may be shared without further reference to legislation.

The figure on the following page summarises the procedures for using Legislation to assess whether data should be shared.

## 2.10 Using Legislation to assess whether to share data



## 3. Consent

### 3.1 Introduction

Not all agencies within the Highland Data Sharing Partnership routinely seek consent for data sharing. The Police Service for example, because it is principally concerned with the detection and prevention of crime, does not generally seek consent to share data. However, for other agencies consent is a basic prerequisite for data sharing. The information in this section is provided so that all agencies will have a broad understanding of the need for consent, how and from whom consent is sought and how consent is recorded. Practitioners must also be familiar with the relevant policies within their own agencies.

Other than in situations involving the prevention of harm or the prevention or detection of crime, data subjects should generally be able to exercise choice to decide whether their data is shared or not. This will be done by asking the data subject to give their consent to data sharing. Where consent is sought, it must represent a genuine free choice for the individual. Consent should not be sought in circumstances where data will probably be shared whether consent is provided or not.

However, where consent is given by a data subject, this greatly simplifies the assessment of whether data should be shared. The giving of explicit consent satisfies the requirements of the Data Protection Act, the Human Rights Act and Scottish common law and statutory responsibilities although the Data Controller is still responsible for ensuring that there is a legitimate need-to-know before sharing data.

### 3.2 What is Consent?

There are two key principles involved in consent as it is applied to data sharing between agencies. These are that consent must be:

- Informed, and
- Explicit

**Informed** consent means that the data subject must understand what is being asked of them and must give their permission freely. This will generally involve providing the data subject with an explanation of the possible consequences of their giving or withholding consent. To facilitate this, practitioners may wish to use the leaflets provided by the Highland Data Sharing Partnership for this purpose (sample leaflets are provided in Appendix C of this document). However, allowing a data subject to read a leaflet is not on its own an adequate means of

ensuring that the data subject is informed. The practitioner must offer an explanation to support the text in the leaflet and must assure themselves that the data subject understands the issues. The leaflet can then be left for future reference.

**Explicit** consent means that the data subject positively gives their consent for data to be shared. Usually this is recorded through the use of a consent form (an example consent form is provided in Appendix B of this document). Implied consent is not sufficient for data sharing. Implied consent simply means that a data subject has not explicitly said that they **don't** agree to their data being shared, so it is inferred that they **do** agree. Implied consent may be appropriate for certain instances of sharing information within an agency (for example, if a nurse weighs a patient, consent would be implied to allow sharing this data with a doctor) but it is not sufficient for data sharing between agencies.

### **3.3 Who Can Give Consent?**

Consent should always be sought from the data subject. Where the data subject does not have the capacity to give consent, a person with power of attorney, guardianship, etc. for the data subject can give consent. Where the data subject is a child too young to give informed consent, a parent or guardian may give consent.

#### **People without the Capacity to give Informed Consent**

In the first instance, consent must be sought directly from the data subject. However, for consent to be informed the data subject must be capable of understanding the issues involved. Where a person does not have the capacity to understand these issues, consent may be sought only from a guardian or person who has power of attorney for the data subject (see Section 2.7, *The Adults with Incapacity (Scotland) Act 2000* for further details). Where a person has a disability, it should not be assumed that they do not have the capacity to give consent for data sharing.

When considering whether a data subject has the capacity to give informed consent, the following issues must be considered;

- Is the data subject capable of making and communicating their choice?
- Does the data subject understand the nature of what is being asked and why?
- Does the data subject have memory abilities that allow the retention of information?
- Is the data subject aware of any alternatives?
- Does the data subject have knowledge of the risks and benefits involved?
- Is the data subject aware that such information is of personal relevance to them?

- Is the data subject aware of their right to refuse, knows how to refuse, and is aware of the consequences of refusal?
- Has the data subject ever expressed their wishes relevant to the issue when greater capacity existed?
- Is the data subject expressing views consistent with their previously preferred moral, cultural, religious, family and experiential background?

Where a data subject does not have the capacity to give informed consent, and another person gives consent on their behalf, this situation must be explained to the data subject.

### **Children and Young People**

Whenever a decision is to be taken about data sharing when a child is involved, the welfare of the child will always be the paramount consideration (for more information see Section 2.4, *The Children (Scotland) Act 1995*).

#### **Children Under the Age of Twelve**

Where the data subject is a child under the age of twelve, consent for data sharing will be sought from a parent or guardian. However, the child has a right to be kept informed and to participate in the process if possible. In circumstances where the practitioner considers a child under twelve to have the capacity to understand informed consent, and where there is difficulty in relationships with parents/carers, a request by the child that consent should not be sought from parents/carers should be respected wherever possible.

#### **Children From the Age of Twelve**

Children from the age of twelve years are presumed to have the mental capacity to give informed consent in their own right. However, where the child is under sixteen, practitioners may also wish to seek consent from parents or carers if there is no reason not to. Where a child is experiencing a breakdown in relationships with parents/carers or where there are safety or welfare concerns, their desire not to seek consent from parents/carers must be respected.

#### **Children From Sixteen to Eighteen**

Parental rights and responsibilities largely cease when a child reaches the age of sixteen. The exception to this is the parent's responsibility to provide guidance to the child until the age of eighteen. Therefore practitioners may wish to share data on young people from age sixteen to eighteen with parents or carers. However, this should normally be done with the consent of the subject or on the basis of the same assessment that would be used to justify the sharing of any other data without consent (see Section 2.2 for further information).

## **People with Parental Responsibilities**

People with parental responsibilities are:

- The child's mother (whether she is married to the father or not)
- The child's father if:
  - he is married to the mother either when the child is conceived or afterwards,
  - he is not married to the mother but he jointly signs the Birth Register with her since 4 May 2006,
  - he is not married to the mother but the mother has agreed he should have parental rights and responsibilities (and this is registered in the Books of Council and Session), or
  - he is not married to the mother but the Sheriff Court or Court of Session has made an order giving him parental responsibilities and parental rights.
- A guardian who has been properly appointed (in the event of the parent's death)

Other adults can hold full parental rights and responsibilities only if this is decided in court.

The law aims to make sure that parents who are separating or divorcing are both involved in bringing up their child and continue to share their responsibilities towards the child. This means that in the event of separation or divorce both parents continue to have responsibilities and rights towards the child.

Parental rights and responsibilities can only be removed by order of the Sheriff Court or the Court of Session.

### **3.4 How to Obtain and Record Consent**

When seeking consent to share data, the practitioner must clearly explain;

- What data may be shared,
- With whom it may be shared, and,
- The purpose(s) for which data may be shared

The practitioner should also explain (with the assistance of the information leaflets if required) the advantages to the data subject of giving consent and the possible disadvantages of withholding consent.

The practitioner must also explain that, even if the data subject does not give consent, in certain circumstances data may still be shared.

Consent should be recorded by the data subject or a parent or legal representative signing a consent form. A sample consent form is provided in Appendix B of this document. When complete, a copy of the consent form and the information leaflet should be left with the data subject for reference.

### **3.5 Sharing Data about an Unborn Child**

Sharing information about an unborn child presents additional challenges. Practitioners involved in the care of a pregnant woman should always consider if the unborn child may be endangered by the mother's condition, behaviour or lifestyle. Where there is a concern about the foetal development and its impact on the child when born or the mother's state of wellbeing, practitioners should try to secure consent from the mother to share data as necessary. This may include sharing information prior to the birth of a child to ensure protective plans are in place from when the baby arrives.

If the pregnant woman refuses to give permission for data sharing, and there are concerns about the welfare of the unborn child, an assessment should be carried out to decide whether data should be shared. This must be done on the same basis that would be used to justify the sharing of any other data without consent (see Section 2.2 for further information). The welfare of the unborn child will always be the paramount consideration.

If a decision is taken to share data about an unborn child without consent, the pregnant woman should be informed.

### **3.6 If Consent is Refused or Withdrawn**

Individuals have the right to refuse to give or to withdraw consent for data sharing. If consent is refused or withdrawn, the individual's right to decide must be respected. However, as previously noted, even where consent is refused, it may still be necessary to share data in certain circumstances. This must be made clear when a data subject is initially asked to give consent and if they withdraw consent.

#### **If Consent is Withdrawn**

Individuals have the right to withdraw consent for data sharing. If consent is withdrawn, the individual's right to decide must be respected, and no further data should be shared. However, consent to share cannot be withdrawn retrospectively. Information that has already been shared cannot be un-shared. If consent is withdrawn, this will apply only to any possible future instances of data sharing.

Where consent is withdrawn, it may still be necessary to share data in certain circumstances, as noted above. This must be made clear when a data subject withdraws consent.

### **3.7 Circumstances in which Consent Should Not be Sought**

Although seeking consent to share may be the first step towards data sharing, there are circumstances where even the act of seeking consent may place a child or other person at risk. Practitioners must be aware of this and must consider whether seeking consent may present a risk. If the assessment is that seeking consent may present a risk, consent should not be sought and this assessment and the reasons for it recorded appropriately.

### **3.8 Sharing Data Without Consent**

In certain circumstances, a practitioner may decide to share data without consent. The circumstances in which this may be done are detailed in Section 2 of this document.

If data is shared without consent, the following information must be recorded;

- The data subject,
- The practitioner sharing the information,
- The person/agency requesting information,
- The reason(s) data was shared, and
- What information was shared.

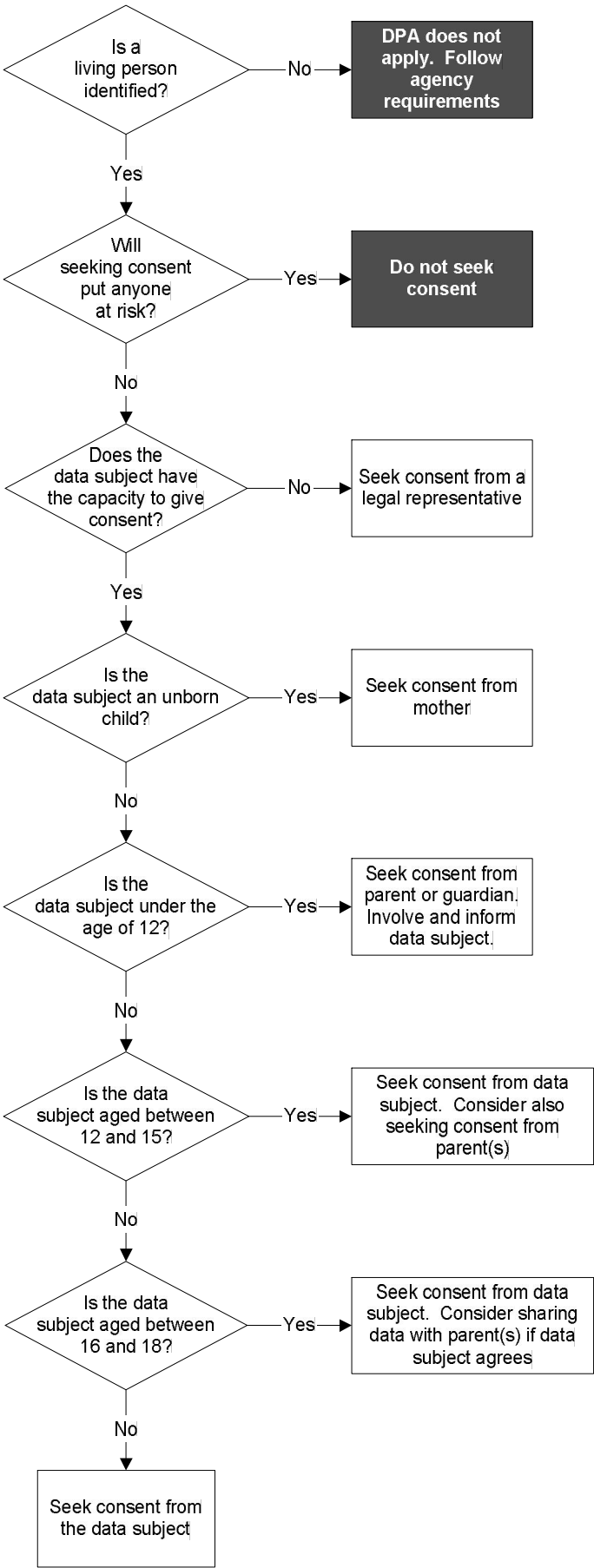
Where it will not cause harm, the data subject should be informed when data about them is shared without their consent.

### **3.9 Summary**

- Consent is not required by all agencies
- Consent must be informed and explicit
- Consent must be given by the data subject, a parent or legal representative
- Consent must be recorded
- If consent is refused or withdrawn, it may still be necessary to share data (the reasons for this should always be recorded)
- Consent should not be sought where this may cause risk (the reasons for this should always be recorded)

The figure on the following page summarises the procedures for seeking consent.

### 3.9 Seeking Consent for Data Sharing



## **4. Methods of Sharing Data**

### **4.1 Introduction**

The seventh Data Protection Principle (see 2.2, The Data Protection Act 1998 for further information) states that all data held by public authorities must be securely processed. When files or electronic data are shared within a single agency, this is relatively simple. When data is shared with another agency, the situation can be more complicated.

The Data Controller must consider how best to share data with other agencies in a timely and appropriate manner while assuring security.

This section describes the main means of sharing data and the most appropriate use for each. These are the minimum standards that must be used by all partner agencies. These requirements do not pre-empt partner agency procedures where these are more rigorous.

### **4.2 Verbal Communication**

If sharing data face-to-face, ensure that this is not done in an area where other people who may not have a need-to-know can overhear.

If sharing information by telephone:

- Do not use a telephone in an area where you may be overheard by other people who may not have a need-to-know.
- Ensure that the person you are talking to is properly identified (calling back to verify this is good practice) and has a need-to-know.
- Do not leave data on answering machines or voicemail.
- Do not use a mobile telephone unless you have no other option. If using a mobile telephone, ensure that this is not done in an area where other people who may not have a need-to-know can overhear.

### **4.3 Written Communication**

Any written communications containing personal information should be transferred in a sealed envelope and addressed by name to the contact in the recipient agency. The contact should be informed that the information has been sent out and should make arrangements with their own agency to ensure both that the envelope is delivered unopened and is received within the expected time scale.

Where an agency or office has a policy that all mail is opened at a central point prior to delivery to a named recipient, then this policy must be made clear to all partner agencies. In these circumstances an alternative means of transfer must be arranged to allow information to be restricted to those who have a need to know.

#### **4.4 E-mail Communication**

Each agency will have procedures for the secure use of e-mail communication. Practitioners must ensure that they are familiar with these procedures.

Sensitive personal data must only be transmitted by e-mail to agencies with secure networks. This means that mail can be sent only to NHSmail (any e-mail address ending with .nhs.net) or to other secure Government domains which have e-mail addresses ending with:

.gsi.gov.uk

.gsx.gov.uk

.gse.gov.uk

.pnn.gov.uk

.scn.gov.uk

.pnn.police.uk

.eu-admin.net

.gsisup.co.uk

.cjsm.net

.psops.net

If it is critical that you send sensitive personal data by e-mail to a recipient in another agency who is not part of a secure network, you must first check with your line manager or supervisor.

#### **4.5 Fax Transfer**

Using fax for data sharing should generally be avoided as it is not secure. In an emergency, and if there is no other possible means of sharing data, fax may be used providing the following steps are taken to make it more secure;

- The recipient should be contacted to confirm the number and to ensure they are aware a fax is about to be sent;
- The recipient should confirm that they are waiting by the fax machine;
- The fax should be provided with a cover sheet stating that the contents are in confidence and that the fax is for the identified recipient only;
- Check fax numbers before dialling - never dial from memory.

- It is good practice to identify frequently used numbers and program these into a fax machine's "memory dial" facility; equally, computer dialling facilities may be used where available. However, numbers must be tested in conjunction with a telephone call before using them for confidential information.
- The fax should be transmitted;
- The recipient should be contacted to confirm receipt.

The fax cover sheet should also provide the name and contact details of the sender and should state that in the event of an error, the sender should be contacted immediately. The amount of information sent via fax transfer should be minimal, and a log of faxes sent out should be kept. Included in this log should be sender and recipient details, date and time of transmission with a copy of the printout from the fax confirming transmission success.

## 4.6 The Government Protective Marking Scheme

The Police Service uses the Government Protective Marking Scheme (GPMS). This scheme is intended to standardise the marking, storage and handling of documents according to a system of classification. This scheme is described here so that practitioners are familiar with the markings on documents produced by the Police Service and understand the implied handling and storage requirements.

Within the GPMS five levels of protective marking are defined. These are:

- TOP SECRET
- SECRET
- CONFIDENTIAL
- RESTRICTED
- PROTECT

Documents may also be marked as "NOT PROTECTIVELY MARKED".

Only documents classified as **NOT PROTECTIVELY MARKED**, **PROTECT**, **RESTRICTED** and **CONFIDENTIAL** will be shared within the agencies of the Highland Data Sharing Partnership.

Documents are classified according to the potential harm that could be done by their compromise.

The compromise of **PROTECT** documents could:

- cause inconvenience or discomfort to individuals
- cause minor disruption to operational effectiveness

The compromise of **RESTRICTED** documents could:

- cause substantial distress to individuals

- make it more difficult to maintain operational effectiveness or security
- prejudice an investigation or make the commission of crime easier
- breach statutory restrictions on disclosure of material
- breach undertakings to maintain confidence of material provided by third parties
- disadvantage public authorities in policy or commercial negotiations

The compromise of **CONFIDENTIAL** documents could:

- prejudice individual security or liberty
- cause damage to the operational effectiveness or security of UK forces, or to the effectiveness of valuable security or intelligence operations
- impede the investigation or make the commission of serious crime easier
- shut down or substantially disrupt significant national operations

The marking applied to each document is applied to the top and bottom of each page. These markings also define how documents should be stored and handled.

**NOT PROTECTIVELY MARKED** documents should be handled and stored in accordance with the usual procedures of the recipient agency.

**PROTECT** documents:

- Must be protected by one barrier (i.e. in a locked desk).
- When sent by post, should be sent in a sealed envelope with no protective marking on the envelope
- May be transmitted by email.
- May be transmitted by fax.

**RESTRICTED** documents:

- Must be protected by one barrier (i.e. in a locked desk) and must not be left unattended on a desk.
- May be copied, but copies must be kept to a minimum
- When sent by post, should be sent in a sealed envelope with no protective marking on the envelope
- May be transmitted by email only to other public authority networks which have formal RESTRICTED accreditation.
- May be transmitted by fax, but only if it is confirmed that the recipient is on hand to receive
- If taken off-site, must be in a locked container and not left unattended

- Must be shredded when no longer required

**CONFIDENTIAL** documents:

- Must be protected by two barriers (i.e. in a locked desk and in a locked office) and must not be left unattended on a desk
- May be copied, but copies must be kept to a minimum
- Must not be discussed on a mobile telephone by voice or text
- When sent by post, must be double enveloped - both addressed. Internal envelope addressed to recipient, external envelope addressed to organisation/dept only. Return address on outer envelope. Protective marking on inner envelope only
- Must not be transmitted by e-mail
- Must not be transmitted by fax
- May only be taken off-site with approval of line manager. Must be protected by two barriers. Must only be viewed in a secure area.
- Must be cross-cut shredded when no longer required.

## **4.7 NHS Confidential Information**

The NHS does not use the Government Protective Marking Scheme. All personal health information i.e. any information relating to health and well-being of an identifiable individual, is classed as confidential. Everyone working in the NHS has a legal, ethical and employment obligation to keep all patient related information confidential unless there are good reasons for sharing that information such as child/adult public protection etc.

All NHS confidential information will be stored securely as outlined in NHS Scotland Standards. NHS staff should refer to their professional code of conduct for further information where relevant.

## **4.8 How to Request Data from Another Agency**

- Locate the correct person to contact in the other agency.
- Contact this person.
- Identify the person and confirm that they are the appropriate source before stating what data you require.
- Explain your need-to-know and the purpose for which you require the data.
- Identify the data subject using their name, address, date of birth and any other relevant information.
- Agree a method for sharing the data.
- Check for any particular handling and storage requirements of the originating agency.

- Record:
  - Why you sought the data
  - What data you were given
  - Who gave it to you
  - The date and time you sought and received the information

You may not pass any data you receive to any third party without the explicit permission of the agency who provided it. You may not use the data received for any purpose other than that given when the information was requested.

## **5. Resolving Disputes**

### **5.1 Introduction**

It is accepted that disputes may arise in the course of managing and sharing data within the Highland Data Sharing Partnership. These may include issues such as:

- Refusal to share data;
- Conditions being placed on sharing;
- Delays in responding to requests for sharing;
- Disclosure of data to practitioners who do not have a genuine need-to-know;
- Failure to follow these procedures;
- The use of data for purposes other than those agreed;
- Inadequate security.

Practitioners must make every effort to work cooperatively to resolve such disputes.

### **5.2 Disputes between Practitioners**

If a practitioner is unable to resolve a data sharing dispute with a practitioner from another agency, they must first raise the issue with their line manager. The line manager will assess whether further action is justified. If it is, the line manager will then make informal contact with the practitioner's line manager at the other agency to try and resolve the issue. If this is not successful the line manager should write to the line manager at the other agency to raise the relevant concerns. If this is not successful then a meeting should be called to try to resolve matters.

If this is not successful, the issue must be referred to the person in their agency who is designated to act as arbitrator for data sharing disputes. A list of these people is provided in the Highland Data Sharing Policy.

Details of disputes resolved in this way must be passed to the Highland Data Sharing Manager. These will then be collated and the results presented to the Highland Data Sharing Partnership. Where appropriate, remedial action will be agreed by the Partnership and fed back to individual agencies.

### **5.3 Complaints from Members of the Public**

The information leaflet provided to data subjects when they are asked for consent also includes guidance on how to make a complaint about data sharing (an example leaflet is provided in Appendix C of this document). In general, complaints from the public will be made if a person believes that their data is:

- inadequate, irrelevant or excessive;
- inaccurate or out of date; or
- kept for longer than is necessary.

Or if they believe that their data has been used, held or shared:

- unfairly;
- for a reason that is not the one it was collected for; or
- without proper security.

If an agency receives a complaint about data sharing, this will be investigated in accordance with that agency's complaints policy. The person making the complaint will be informed of the results of this investigation. If any disciplinary action is required as a result of the complaint, this will be an internal matter for the agency concerned.

If the member of the public making the complaint does not feel that it has been dealt with satisfactorily by the agency concerned, they have the right to take it to the Information Commissioner's Office (ICO). The ICO will then make a judgement based on interpretation of the Data Protection Act.

However, it is also important that details of complaints relating to data sharing are collected across the Partnership. To enable this, each agency must record details of these complaints and their outcomes and pass them to the Highland Data Sharing Manager. These will then be collated and the results presented to the Highland Data Sharing Partnership. Where appropriate, remedial action will be agreed by the Partnership and fed back to individual agencies.

## 6. Summary of Key Points

### Legislation

- Legislation does not prevent data sharing. It provides a framework within which data sharing can be done securely, appropriately and proportionality.
- Legislation helps to weigh benefits and risks.
- Legislation is based upon common-sense principles.

### Consent

- Consent is not required by all agencies or in all circumstances
- Consent must be informed and explicit
- Consent must be given by the data subject, a parent or legal representative
- Consent must be recorded
- If consent is refused or withdrawn, it may still be necessary to share data
- Consent should not be sought where this may cause risk

### Methods

- Always identify the person you will be communicating with.
- Don't give verbal information where you can be overheard
- Don't leave information on answering machines or voicemail.
- Be aware of your e-mail policy
- Don't use fax at all if possible. If there is no alternative, make sure the recipient is standing by to collect the fax.
- Be aware of the Government Protective Marking Scheme and the obligations it places on you.

# Appendix A The Six Caldicott Principles

The Caldicott Report addressed specific issues for health organisations to ensure that patient confidentiality is not undermined.

**Principle 1: Justify the purpose(s).**

Every proposed use or transfer of patient-identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed by an appropriate guardian.

**Principle 2: Do not use patient-identifiable information unless it is absolutely necessary.**

Patient-identifiable information items should not be used unless there is no alternative.

**Principle 3: Use the minimum necessary patient-identifiable information.**

Where it is necessary to identify the patient, you should use the minimum information required. For example, could just an NHS number be used or surname and date of birth?

**Principle 4: Access to patient-identifiable information should be on a strict need to know basis.**

Only those individuals who need access to patient-identifiable information should have access to it, and they should only have access to the information items that they need to see.

**Principle 5: Everyone should be aware of their responsibilities.**

Action should be taken to ensure that those handling patient-identifiable information- both clinical and non-clinical staff - are aware of their responsibilities and obligations to respect patient confidentiality.

**Principle 6: Understand and comply with the law.**

Every use of patient-identifiable information must be lawful. Someone in each organisation should be responsible for ensuring that the organisation complies with legal requirements.

# Appendix B Sample Consent Form



## MULTI-AGENCY CONSENT FORM

To provide services it may be necessary for professionals from public authorities to share information about you. This will only be done if necessary and all agencies will keep this information confidential. By signing this form you agree to your information being shared with this way. You do not have to agree to this, but if you do not, it may take longer to provide services and you may have to provide the same information to several agencies.

I understand that my information may be shared by agencies concerned with providing services for me. By signing this form, I agree to relevant information being shared between professionals if necessary.

Name of Service User (Print): \_\_\_\_\_

Signature of Service User: \_\_\_\_\_

Date of Birth: \_\_\_\_\_ Date: \_\_\_\_\_

Name of Parent or Legal representative: \_\_\_\_\_

Signature of Parent or Legal representative: \_\_\_\_\_

Status: \_\_\_\_\_ Date: \_\_\_\_\_

Even if you do not give consent for your information to be shared, this may still be done in certain circumstances (for example, to prevent or detect crime or to protect a child).

Further information can be found in the following leaflets:

Data Sharing within Integrated Services for Children and Young People: A Guide for Parents and Carers

Data Sharing within Integrated Services for Adults: A Guide for Adult Service Users

# Appendix C Sample Information Leaflets

## **Introduction**

Health, Education, Police and Social Care Staff aim to make sure that the care and support your child receives is planned, tailored and delivered to meet their individual needs. When staff from different practices are working together to arrange the services your child requires they may need to share information. Any information held about your child is kept securely in a file or on electronic information system.

Before this information is shared we may need consent to do so. The staff asking permission will explain what this means before asking for consent.

## **Why do we need to share your child's information?**

- We will share your child's information in order to deliver services in an integrated manner. this is sometimes known as integrated assessment.
- We share your child's information so that neither you nor your child will be asked the same basic questions over and over again by different staff. This reduces the frustration of repeating information.
- It ensures that your child receives co-ordinated treatment and services, since relevant staff have basic information about your child's circumstances.
- If required, it will make easier and quicker access to equipment and adaptations that assist your child with daily living. It may also reduce delays in the provision of care services
- There may be times when we need to share your child's information to ensure their safety.

## **What information about your child will we share?**

- Integrated assessment information. This includes information that will be gathered during the assessment of your child's needs. The type of information shared will depend upon your child's particular circumstances, although this will include general information such as name, address and other professionals involved in your child's care.
- If your child requires social, educational or health care support, a team of professionals will assess your child's needs and will develop a care plan for your child.
- The care plan records information about your child's needs and areas of difficulty. This will help to decide the most appropriate treatment, care and support needed for your child's care.

## **Who will this information be shared with?**

- Your child's information will be shared with the people directly involved in their care and who have a genuine need to be informed e.g. nurses, GP's, social care services, occupational therapy, physiotherapy and other professionals who work with your child.
- Consent will be sought prior to your child's information being shared with other professionals involved with their care.

## **How do we do this?**

- Your child's information will be shared on paper, verbally or on electronic information systems, subject to consent being given.
- Some of your child's information can be held across health care, social care and education records.

- All staff are required to keep written records of their work.

## **Who gives consent?**

- For children over the age of twelve, consent will usually be sought from the individual themselves
- For children under twelve, consideration will be given to their age and level of understanding. If your child understands the nature and consequences, consent will be sought from the child. If not, consent will be sought from the person with legal authority to act on the child's behalf.
- Where a child is over twelve but does not have the capacity to make an informed decision, consent will be sought from the person with legal authority to act on the child's behalf. This could be a parent, guardian or other person with parental rights

## **You can decide not to share your child's information**

- If you do not wish this information to be shared in the way described in this leaflet, make this clear to the person carrying out their care and/or learning plan.
- Very sensitive information may not be shared in some circumstances. You or your child may also choose not to share this type of information.
- If we feel that there is an immediate risk, we can share their information without consent, enabling us to deal quickly with any potential situation e.g. child protection issues or emergency medical procedures when parents are not present.

## Your rights

At any time you or your child have the right to refuse to have information shared. However, this may cause delays in getting services organised and means that you or your child could be asked for the same information repeatedly by different people.

You have the right to request access to information held about your child.

Your child has a right to the respect for their privacy and all staff involved in their care have a duty of confidentiality governed by:

- The Data Protection Act 1998
- The Human Rights Act 1998
- Contracts of staff employment
- Professional codes of conduct
- Common Law Duty of Confidentiality

## Some ways to find out more

Further information can be accessed from [www.nhshighland.scot.nhs.uk](http://www.nhshighland.scot.nhs.uk)  
[www.highland.gov.uk](http://www.highland.gov.uk)

Copies of leaflets can be found in libraries and Council Offices.

Should there be an identified need, this leaflet will also be made available in Braille and languages other than English. Information can also be found in the following leaflets:

- How the NHS protects your health information
- How to see your Health Records

Or by contacting:

NHS Highland  
Data Protection  
Assynt House  
Beechwood Park  
Inverness IV2 3HG  
Phone: 01463 717123  
Website: [www.nhshighland.scot.nhs.uk](http://www.nhshighland.scot.nhs.uk)

## Any Queries?

If you have any queries regarding any part of this leaflet, please feel free to contact your key worker or associated professional.

## Complaints

If you wish to make a complaint about how your information is shared or about anything in this leaflet, please contact your key worker or associated professional.



# INFORMATION SHARING WITHIN INTEGRATED SERVICES FOR CHILDREN & YOUNG PEOPLE A Guide for Parents and Carers

The Highland Data Sharing Partnership  
recognises the work of the pan-Grampian  
eCare Project

## Your rights

At any time throughout the process you have the right to refuse or withdraw consent to have your information shared. However, this may cause delays in getting services organised and means that you could be asked for the same information repeatedly by different people.

You have the right to request access to information held about you

You have a right to the respect of your privacy at all times and all staff involved in your care have duties of confidentiality governed by:

- The Data Protection Act 1998
- The Human Rights Act 1998
- Contracts of staff employment
- Professional codes of conduct
- Common Law Duty of Confidentiality

## Some ways to find out more

Further information can be accessed from  
[www.nhshighland.scot.nhs.uk](http://www.nhshighland.scot.nhs.uk)  
[www.highland.gov.uk](http://www.highland.gov.uk)

Should there be an identified need, this leaflet will also be made available in Braille and languages other than English. Information can also be found in the following leaflets:

- How the NHS protects your health information
- How to see your Health Records

Or by contacting:

NHS Highland  
Data Protection  
Assynt House  
Beechwood Park  
Inverness IV2 3HG  
Phone: 01463 717123  
Website: [www.nhshighland.scot.nhs.uk](http://www.nhshighland.scot.nhs.uk)

## Any Queries?

If you have any queries regarding any part of this leaflet, please feel free to contact your key worker or associated professional.

## Complaints

If you wish to make a complaint about how your information is shared or about anything in this leaflet, please contact your key worker or associated professional.



# INFORMATION SHARING WITHIN INTEGRATED SERVICES FOR ADULTS

## A Guide for Adult Service Users

The Highland Data Sharing Partnership  
recognises the work of the pan-Grampian  
eCare Project

## Introduction

Health, Housing, Police and Social Care Staff across the NHS Highland area aim to make sure that the care and support you receive is tailored, planned, and delivered to meet your individual needs. When staff from different practices are working together to arrange the services you require, they may need to share information about you. Any information held about you is kept securely in a file or on electronic information systems.

Before your information is shared we may need your permission to do so. The staff asking your permission will explain what this means before asking for your consent.

## Why do we need to share your information?

- We share your information so that you don't need to be asked the same basic questions over and over again by different health and care staff. This reduces the frustration of repeating information
- It ensures that you receive co-ordinated treatment and services since relevant staff involved in your care have basic information about your circumstances
- It will make easier and quicker access to equipment and adaptations that assist you with daily living
- It may also reduce delays in the care services we provide
- Sometimes we need to share your information to ensure your safety

## What information will we share?

- At present, this will be information gathered during the assessment of your needs. This is known as the Single Shared Assessment
- If you require social or health care support, the first professional you see will find out what you need and will record information on the Single Shared Assessment form
- The form records information about you, your needs and areas of difficulty in order to help decide the most appropriate treatment, care and support for you
- This information is used to help plan your care
- A copy of the assessment is given to you in the language and format of your choice
- You will be asked if you agree to it being shared with other professionals involved with your care
- Very sensitive information may not be shared in some circumstances

## Who will this information be shared with?

- Your information will be shared with the people directly involved in your care and who have a genuine need to be informed e.g. nurses, GPs, social care services, occupational therapy, physiotherapy and

anyone else with whom you have agreed that we may share it

- Your information will only be shared with other people who provide services to support you

## How do we do this?

- Your information will then be shared on paper, verbally or on electronic information systems
- Some of your information may be held in health care records, and some in social care records. All staff are required to keep written records of their work

## You can decide not to have your information shared

- If you do not wish your information to be shared in the way described in this leaflet, make this clear to the person carrying out your assessment
- You can also choose not to share this type of information. We will respect this decision

## What if someone is not able to decide themselves?

- If a person is not able to make a decision about their information being shared, only a legally appointed representative can do so on their behalf
- This person can be:-
  - Their agent (confirmed by a letter of consent from the service user)
  - A person with a (welfare) Power of Attorney
  - A representative appointed by the court under the terms of the Adults with Incapacity (Scotland) Act 2000.

## Why share information?

You may have people helping you with things that are going on in your life. It may be a teacher, youth worker, social worker or maybe a school nurse or a local police officer.

To help you and to arrange services and support for you, they may need to share information about you.

This leaflet explains why and how information may be shared.

## What information about me will be shared?

**Only information that is needed by other people to give you the support, care or protection you need.** This may be:

- your name
- where you live
- the people around you
- what you need
- any help you already have

## Who will see my information?

Only the people involved in helping and supporting you. This may be just one person or perhaps a group of people, depending on your needs.

## Will I be asked?

Whoever asks you, should explain exactly why they want to share information and what will happen as a result.

**If you are over 12**, usually you will be asked to agree to information about you being shared.

**If you are under 12**, usually you will be involved in the decision, but your mum or dad or the person may be asked to agree too.

You may be asked to sign a 'Consent Form'. This shows that you agree to your information being shared between agencies.

## Can I refuse to share my information?

**YES** – but this might slow down getting the care or support you need. For example, if staff can't share information between them, they will each have to ask you for details.

**BUT** – if you or someone else is thought to be at risk of harm, information may have to be shared between staff.

## Will my parents be told?

Not necessarily. But usually you and your parents would be involved in getting you the help you need.

You may be asked to agree that information about you is shared with your parents. If staff decide that information needs to be shared with parents or carers, you will usually be told what information was shared.

## What will happen to the information that is shared?

It will be kept carefully on a data base or on paper. Only those who are helping you will be able to see any information about you.

The details will be used to make sure that you can get the help you need.

Laws prevent workers passing on information without agreement (unless they think you are at risk of harm).

## More questions to ask?

Ask the people who support you – like your family, carers, social worker, teacher, school nurse.

They should be able to answer your questions or to find out more for you.

## Need help with understanding this leaflet?

If you want this information in another language, audio or large print, please ask your teacher, social worker or school nurse.

getting  
it right  
for every child

# YOU AND YOUR INFORMATION

*A guide for young people  
and children  
about  
information sharing*



## Appendix D References

### **Highland Council specific guidance:**

Highland Policy for Sharing Information

<http://ntintra1/cx/infomanagement/data-sharing/info-sharing-document.pdf>

Data Sharing Guidance

<http://ntintra1/cx/infomanagement/data-sharing/data-sharing-guidance.htm#info-sharing>

Child Protection Policies for your Community Group (2003)

[http://ntintra1/cx/pdf/child\\_protection\\_policy.PDF](http://ntintra1/cx/pdf/child_protection_policy.PDF)

### **NHS Highland specific guidance:**

NHS Code of Practice on Protecting Patient Confidentiality

<http://www.nhshighland.scot.nhs.uk/Your%20Rights/code%20of%20practice%20on%20maintainin%20confidentiality.pdf>

Data Protection Policy

Staff Handbook and Induction Process

The Caldicott Principles

Sharing Information about Children at Risk

Chief Medical Officer letter and Brief Guide, 2004

<http://www.scotland.gov.uk/Publications/2004/09/19924/42748>

Confidentiality – it's your right

<http://www.nhshighland.scot.nhs.uk/Your%20Rights/Confidentiality/Confidentiality%20leaflet%20Highland.pdf>

### **General Guidance:**

Sharing Information About Children At Risk, Scottish Executive (2003)

<http://www.scotland.gov.uk/Publications/2004/04/18512/28931>