Information Sharing Procedures

Version 3.3

Policy Reference: ISP Information Sharing Procedures – Version 3.3	
Prepared by: ISP review group of DSP	**Date of Issue:** March 2013
Lead Reviewer: Area Information Security Manager, NHS Highland	**Date of Review:** March 2015

Distribution

- NHS Highland – Aileen Fraser
- Northern Constabulary – Ian Williams
- Highland Council – Miles Watters
- Argyll and Bute Council – Iain Jackson
- HIFRS – Antony Gardner
- Third sector – Les Hood

Change History

Version	Date	Changes	Initial
1.9	01/05/2008	First issue	SM
2.0	26/11/2010	Second issue	SM
3.0	02/11/2011	Third issue	SM
3.1	04/12/2012	Fourth issue	SM
3.2	07/02/2013	Fifth issue	SM
3.3	06/03/2013	Sixth issue	SM

Foreword

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 Argyll and Bute 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.

CONTENTS

1. Overview and Purpose

1.1 Introduction

Before sharing any personal data you hold, you need to consider all the implications of doing so. Your ability to share data is constrained by a number of factors which include the Data Protection Act, statutory prohibitions and/or a duty of confidence. However, effective integrated working requires timely, proportionate and appropriate data sharing.

Many types of planned, regular data sharing are covered by Data Sharing Agreements (more information is provided in Section 5.9). Each partner agency should maintain a register of Data Sharing Agreements which practitioners can search. Data Sharing Agreements describe how, when, why and with whom data should be shared for specified purposes. Where sharing is covered by a Data Sharing Agreement, you should refer to the agreement for guidance. In situations which are not covered by a Data Sharing Agreement, these procedures will guide you through the process of deciding what to share and who to share it with. These procedures are applicable to all practitioners involved in sharing data within the Highland Data Sharing Partnership area. They apply equally to those practitioners who are asked to share data and to those who have data which needs to be shared.

1.2 Purpose

Effective data sharing requires practitioners to make decisions balancing the right to privacy and confidentiality against the need to share information with other agencies and services. The purpose of these Procedures is to provide a framework describing briefly;

- When to share data, including the role of consent,
- What to share and who is responsible for shared data,
- Who to share with and the role of disclosure,
- How to share securely,
- How to resolve disputes.

This is overarching guidance on data sharing and is underpinned by professional guidance on specific areas of information sharing.

1.3 Definitions

Within these procedures the following definitions are used:

Anonymised Information means information from which no individual can be identified.

Data Controller means a person (normally at CEO level) who determines on behalf of an organisation the purposes for which, and the manner in which, data is processed and shared. The data controller is responsible for ensuring that data processing within their organisation complies with the requirements of the Data Protection Act.

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 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.

Data Subject means the person user to whom data refers.

Highland Data Sharing Partnership means the partnership comprising Highland Council, Argyll and Bute Council, Northern Constabulary, Strathclyde Police, NHS Highland, Inverness Prison, High Life Highland, Strathclyde Fire and Rescue Service and Highlands and Islands Fire and Rescue Service.

Personal Data means data relating to a living individual who can be identified;

a) from that data, or
b) from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Personal health information means any information relating to the health and well-being of an identifiable individual.

Public Authority as defined in section 3 of the Freedom of Information (Scotland) Act 2002 means;

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

Sensitive Personal Data, as defined in Part 1, Section 2 of the Data Protection Act 1998, 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.

1.4 Overview of data sharing

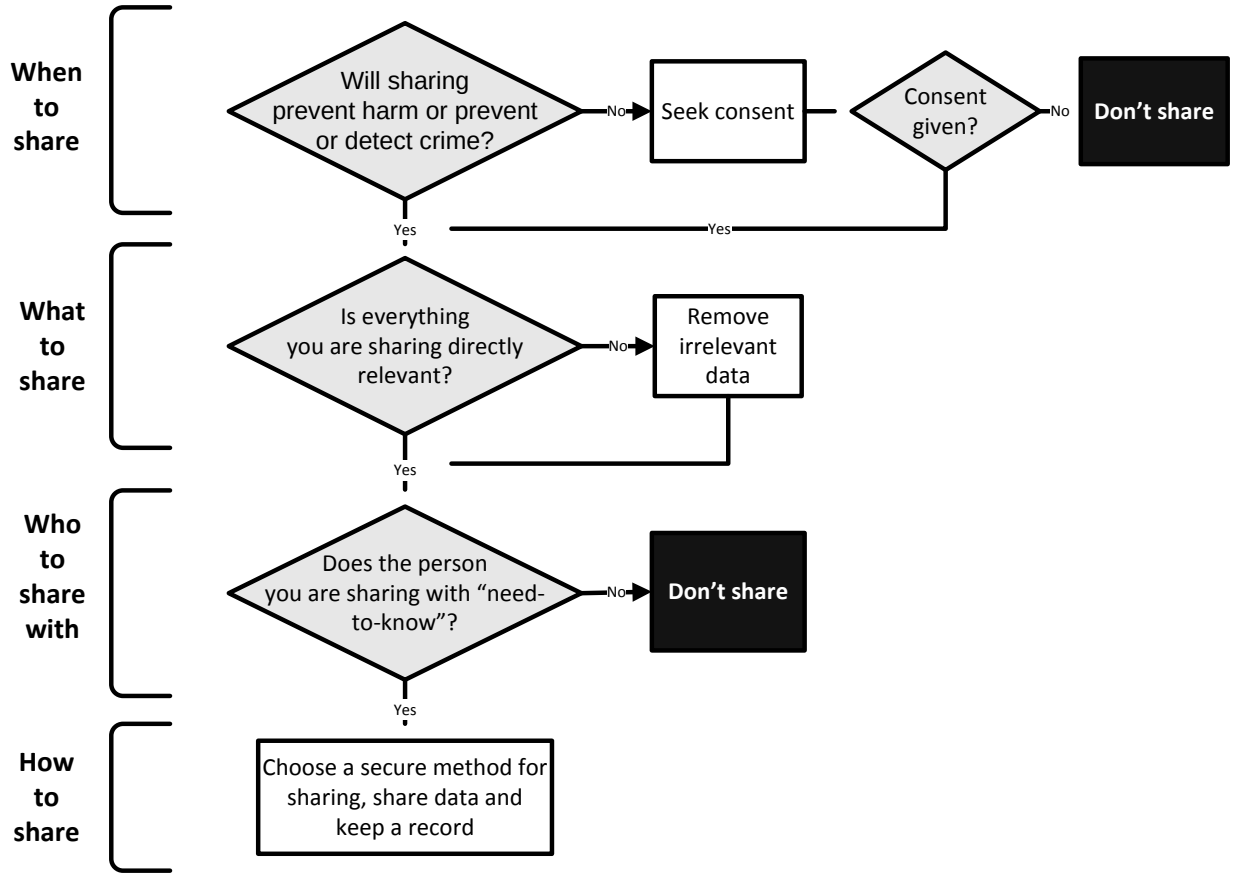
The decision whether to share information with another agency or service generally rests with the practitioner. Practitioners must balance the requirement to comply with legislation and agency rules and the need to share information in order to provide a more effective service.

The first step when considering whether to share information is to find out whether a Data Sharing Agreement exists which relates to the purpose for which you are sharing. Data Sharing Agreements generally cover regular, planned information sharing. If an agreement exists, you must follow the guidance provided there.

However, there are circumstances where it may be necessary to share data but a Data Sharing Agreement is not available. In these circumstances there are four simple, clearly defined steps which each practitioner should go through when considering whether to share information. Provided these steps are followed, practitioners can be assured that they are sharing appropriately. The steps are;

> **When to share.** In what circumstances is it appropriate to share information? Do I need to ask for consent?
> **What to share.** What information is it appropriate to share?
> **Who to share with.** Who can I share information with? What is the role of Disclosure?
> **How to share.** What means should I use to send information securely to another service or agency?

These steps are described in this Procedure and summarised in the Information Sharing Leaflet. The diagram below summarises the process of sharing data.



1.5 The Data Protection Act

In the UK the main piece of legislation relating to data sharing is the Data Protection Act 1998 (DPA). This came into force in the UK in 2001 and 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 covers much more than data sharing; it covers most aspects of how organisations are required to store and handle information. To find out more about the DPA, use the following link to the ICO website;

http://www.ico.gov.uk/for_organisations/data_protection_guide.aspx

There is a common misconception concerning the DPA. This relates to the term "*data*". Some people believe that the term data (and therefore the DPA) applies only to electronic data. This is incorrect. The terms "*data*" and "*information*" are used interchangeably in the DPA. Legislation (and this guidance apply) equally to the sharing of information in any format whether it's electronic, written or verbal.

1.6 The role of Caldicott Guardians

Each NHS organisation is required to have a Caldicott Guardian. Acting as the 'conscience' of an organisation, the Guardian actively supports work to enable information sharing where it is appropriate to share, and advises on options for lawful and ethical processing of information.

The Guardian plays a key role in ensuring that NHS and partner organisations satisfy the highest practical standards for handling patient identifiable information. Each Guardian is responsible for ensuring that the six principles identified in the Caldicott Report are applied. The principles are;

Principle 1: **Justify the purpose(s).**
Principle 2: **Do not use patient-identifiable information unless it is absolutely necessary.**
Principle 3: **Use the minimum necessary patient-identifiable information.**
Principle 4: **Access to patient-identifiable information should be on a strict need to know basis.**
Principle 5: **Everyone should be aware of their responsibilities.**
Principle 6: **Understand and comply with the law.**

1.7 Other legislation and codes of practice

Other items of legislation and codes of practice affect data sharing in the UK.

Please note that other National legislation and common law requirements relate to data sharing. This is a developing topic. If you are unsure about the legislative context for data sharing, speak to your organisations' Data Protection Officer and/or look at the website of the office of the Information Commissioner;

http://www.ico.gov.uk

2 When to share

2.1 The basis for sharing

Personal data, sensitive personal data and personal health information should only be shared with another service or agency when there is an identified need to do so.

Information must be shared where this will prevent harm to the individual or a third party and where it will assist in preventing or detecting crime.

2.2 Consent

Asking for a data subject's consent is an important part of the process of data sharing. However, it is not appropriate to seek consent in every situation. For example, where data is shared to prevent harm or to prevent or detect crime, consent is not required.

It is important that when we do ask for a data subject's consent, this is only done when we are offering a real choice. Consideration must be given to the purpose for which data will be shared. If this is to prevent harm or to prevent or detect crime, the information will be shared regardless of the agreement of the data subject. In these circumstances, we should not ask for consent because we wouldn't be offering a real choice – if the data subject refused to give consent, the information would still be shared.

When sharing without consent it is good practice to inform the data subject, though there is no legal obligation to do this. In cases where informing the data subject could put someone at risk or might impact a police investigation, this should not be done.

Information which is anonymised, i.e. statistical data, or other data from which the identity of the data subject cannot be inferred, can be shared without asking for consent.

Where there is a need to share information, but this is NOT being done to prevent harm or to prevent or detect crime, the data subject should be asked for consent. If consent is not given, information should not be shared. Consent must be informed. That is to say that the data subject must understand what is being asked for. To ensure this the following should be explained when asking for consent;

The purpose of the information sharing,
What information will be shared and with who,
What the effect will be if information is/is not shared.

Appendix B provides examples of leaflets which may be given to data subjects to help them understand these points.

If given, the consent of the data subject must be recorded. This may be done on the consent form provided as Appendix A to this procedure, or by using another agency consent form.

2.3 Who can give consent?

Where possible, consent should be sought directly from the data subject. However for consent to be informed, the person giving consent must be capable of understanding the issues involved. Where a person is too young or does not have the capacity to understand these issues, consent may have to be obtained from another person.

Where the data subject is a child under the age of twelve, consent should 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 the issues of 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 years are presumed to have the mental capacity to give informed consent in their own right.

Where for any reason a person does not have the capacity to understand the issues of consent, consent may be sought only from a guardian or person who has power of attorney for the data subject.

2.4 Withdrawal of consent

Having given consent to share information, individuals have the right to withdraw that consent at a later date. If consent is withdrawn, the individual's right to decide must be respected. However it must be made clear that;

- Information which has already been shared cannot be "unshared". It will continue to be available in other agencies with whom it has already been shared. The withdrawal of consent will only apply to information which might have otherwise been shared after consent is withdrawn.
- Data Subjects have the right, under Section 10 of the Data Protection Act 1998, to request that an organisation stops processing data held about them. Where an agency is in possession of shared data and consent to share has been withdrawn, that agency will have a duty to consider requests received under Section 10 and respond appropriately within 21 days.
- Even if consent is withdrawn, it may still be necessary to share data in certain circumstances, for example to prevent harm or to prevent or detect crime.

3 What to share

3.1 Deciding what to share

In each case where data sharing is required, it is the responsibility of the practitioner involved to decide what specific information should be shared. In overarching guidance such as this it is not possible to be prescriptive in terms of defining what should be shared in every case. Instead, practitioners are required to apply the principles of relevance and proportionality when they are considering data sharing.

It is also the responsibility of the practitioner to ensure that information which is shared is accurate and up-to-date.

3.2 Relevance

Only information which is relevant to the objectives of the current instance of data sharing should be shared. The judgement of what is relevant rests with the practitioner. Often this will involve looking at the past history of a data subject and deciding what is actually relevant to the current situation. This may not always be clear-cut and will require the application of professional judgement.

3.3 Proportionality

The minimum amount of information required to achieve the objectives of the current instance of data sharing should be shared. The judgement of what is proportionate rests with the practitioner.

3.4 Responsibility

Data is the responsibility of the service or agency which originally obtained it from the data subject. If this is shared with another service or agency, the information is still the responsibility of the originating agency. This is significant for two reasons;

> If information is shared with another agency or service, they may not share this information further without the explicit permission of the originating agency.
>
> Responsibility for the security of data remains with the originating agency, even when this data is shared with other agencies.

3.5 Retention

The DPA places obligations on organisations in terms of retention of data. In particular, the DPA requires that organisations retain client data only while it is necessary to do so. Information which is no longer required must be deleted. The same principle applies to shared data. Shared data must be retained only while it is required to support the purpose of the data sharing. When it is no longer required, shared data must be deleted from electronic systems and/or paper copies must be securely destroyed.

3.6 Reuse and Secondary (Tertiary) Processing

The most fundamental concepts within the Data Protection legislation are that all processing of personal information (which includes sharing) must be (1) done in a manner which is both fair to the Data Subject and (2) done for a specified and lawful purpose.

If you wish to use or disclose personal data for a purpose that was not contemplated at the time of collection (and therefore not specified in a privacy notice), you have to consider whether this will be fair. If using or disclosing the information would be unfair because it would be outside what the individual concerned would reasonably expect, or would have an unjustified adverse effect on them, then you should regard the use or disclosure as incompatible with the purpose you obtained the information for.

In order to avoid the requirement of having to obtain such additional consents, organisations should always consider whether they can actually use properly anonymised data rather than raw personal information or whether there is an alternative way of obtaining the necessary output.

http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/anonymisation.aspx

4 Who to share with

4.1 The need-to-know

It is not possible to provide a prescriptive list of who information should be shared with in every circumstance. Instead, the principle of need-to-know must be used when deciding who to share information with. This means that information must only be shared (with or without consent) with people who have an identified need-to-know. This is defined as people who have a public agency function (including commissioned services from the third sector) and who need the shared information in order to do their job. Information may not be shared with any person who does not have an identified need-to-know. It is the responsibility of the practitioner to ensure that any person with whom they are sharing has an identified need-to-know. This includes taking steps to confirm the identity and role of any person who asks for information.

4.2 Disclosure

Many people conflate consent and disclosure, but the two are significantly different and separate processes. Consent is the process of asking the data subject for permission to share their data. Disclosure is the process where a practitioner satisfies themselves that sharing is necessary and appropriate. Disclosure must be undertaken whether sharing is done with or without consent. Disclosure is based on the answers to three questions;

> **The need-to-know**. Is the information being shared only with people who have an identified need-to-know?
> **Relevance**. Is the information being shared directly relevant to the purpose of the proposed data sharing?
> **Proportionality**. Is the information being shared the minimum required to achieve the purpose of the proposed data sharing?

Only when the practitioner is satisfied that the answer to these three questions is yes may data be shared. Most agencies have procedures for recording the fact that the disclosure process has been completed.

4.3 Record keeping

From the information provided in this guidance, it will be obvious that there is no single “right” answer to the question of whether it is appropriate to share data. Each case must be judged on its’ own merits. As part of their day-to-day work practitioners are required to make reasoned judgements balancing the right to privacy and confidentiality against the need to share information to prevent harm and to provide better services. As it is possible that a practitioner may later be required to explain a particular judgement about data sharing, it makes sense that clear records should be kept. Many line-of-business applications support this and in general this record should include;

> The identity of the data subject(s).
> The date of sharing.
> The purpose of data sharing.
> Whether consent was sought and given (and the reasons if it was not).
> What information was shared.
> Who it was shared with.
> The method used for sharing.

These records do not usually have to be extensive or detailed. Their purpose is simply to act as an aide-memoire to assist the practitioner if they are asked later to explain a particular instance of data sharing.

5 How to share

5.1 Introduction

When there is an identified need to share information, it's often important that this is done quickly. However, the information being shared may include very sensitive personal details, so it is also important that sharing is done securely. This section looks at the principal methods of sharing and provides guidance on how to make these secure.

This section provides overarching guidance on methods of sharing data. However, this section does not pre-empt procedures in place in individual agencies or services.

5.2 Verbal Sharing

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

If sharing by telephone:

- Do not use a telephone in an area where the call may be overheard by other people who may not have a need-to-know.
- Ensure that the other person 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 there is 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.

5.3 Sharing on paper

Paper records which include personal information must never be left unattended, particularly in a public place and must not be read or left visible in a public place where they may also be read by a person who does not have an identified need-to-know (for example, on public transport).

If paper records which contain personal information are lost or stolen, this must be reported immediately to the relevant agency department.

Paper records which contain personal information and which are no longer required must be destroyed securely (i.e. by shredding or passing to a secure disposal point). Paper records which contain personal information must never be disposed of by placing with general refuse.

If paper records are shared with individuals by postal services, it should be noted that Royal Mail Recorded Delivery items, or items too big to fit through a letter box, may be left with a neighbour. For this reason Royal Mail Recorded Delivery must not be used for the posting of sensitive data and packages containing sensitive data which are too big to fit through a letter box must not be sent using Royal Mail services. These restrictions only apply to mail sent to individuals, not mail sent to agencies, services or organisations which have arrangements in place for the receipt of mail.

5.4 Using e-mail to share

E-mail is a popular method for sharing information between agencies and services. E-mail is quick, convenient and simple to use. However, not all e-mail is secure, and practitioners must be aware of the limitations of sharing information in this way.

Most personal e-mail is sent via the Internet. This is not secure as e-mails sent via the Internet can be intercepted or redirected and read by someone other than the intended recipient. However, public sector agencies have access to secure e-mail which is not sent via the Internet. This secure e-mail is transmitted via a special network known as the Government Secure Extranet (GSX). These secure e-mails don't look any different to non-secure emails and are sent, received and read in the normal way.

For an e-mail to be sent using GSX, both the sender and the recipient must be linked to this special network. This can be confirmed by looking at the e-mail address. Addresses ending with the following are linked to GSX;

.nhs.net
.gsx.gov.uk
.gsi.gov.uk
.gse.gov.uk
.pnn.gov.uk
.pnn.police.uk
.scn.gov.uk
.gsisup.co.uk
.cjsm.net
.psops.net

When a user has a secure e-mail address, and sends or forwards an e-mail to an address that ends in one of the above, the e-mail will be sent automatically via GSX. If the recipient replies, the reply will also automatically be sent via GSX. This also applies to those public sector employees who have two e-mail addresses, one secure and one non-secure. So, for example, Highland Council practitioners may have two e-mail addresses; *recipient.name@highland.gov.uk* is not secure while *recipient.name@highland.gsx.gov.uk* is secure. When a user who has two e-mail addresses sends an e-mail to another secure address, the e-mail will automatically be routed via their GSX address.

Where e-mail is being sent from an external organisation to a user who has two e-mail addresses, it's important to ensure that sensitive information is always sent to the secure address.

Password protecting attachments to e-mail is not an acceptable substitute for using secure e-mail.

Manual or automatic forwarding of e-mail from a secure to a non-secure e-mail address (i.e. forwarding work e-mail to a home e-mail account) must not be done where the forwarded e-mail may contain personal information.

Sending an e-mail from an unsecure to a secure address does not provide security. For e-mails to be secure, both the person sending and the person receiving the e-mail must have secure e-mail.

It should be noted that some Highland Council Education staff use the Glow system for e-mail. Glow e-mail addresses use the format *recipientname123@highlandschools.org.uk*. These e-mail addresses are not part of the GSX system and are not secure. They must not be used for the transmission of sensitive data.

It should also be noted that some third sector users have been provided with NHSMail accounts. These addresses take the same form as other NHS e-mail addresses, i.e. *recipient.name@nhs.net*. These e-mail addresses are secure and may be used for the transmission of sensitive data.

A dedicated secure e-mail link is provided between Highland Council and Highlands and Islands Fire and Rescue Service. All e-mails between these two organisations are automatically routed via this link and are secure.

If there is any doubt about whether e-mail senders or recipients have access to GSX, agency IT departments will be able to provide further information.

5.5 Using fax to share

Using fax for sharing sensitive information 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 precautions are taken;

- 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.

5.6 Using laptops and portable data storage devices

Laptops, tablets and other portable computers may contain personal data and may be used to share this data. If a laptop or tablet is used in this way;

- Never leave the computer unattended,
- Don’t use the computer in a public place where people who don’t have a need-to-know can read the screen.

Laptops, tablets and portable storage devices such as memory sticks which are used to store personal data must be encrypted. This ensures that even if these items are lost or stolen, unauthorised users cannot access the information contained on them.

If there is any doubt about whether a computer or memory stick is encrypted, agency IT departments will be able to provide further information.

Any loss or theft of any electronic device containing personal data must be reported immediately to the relevant agency department.

5.7 The Government Protective Marking Scheme (GPMS)

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 three relevant levels of protective marking are defined. These are:

- CONFIDENTIAL
- RESTRICTED
- PROTECT

Documents may also be marked as "NOT PROTECTIVELY MARKED". These markings may be applied to hard copy (i.e. paper copies) as well as electronic documents. The handling and storage requirements for these documents are as follows;

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 secure email only.
- 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.

5.8 NHS Confidential Information

The NHS does not use the Government Protective Marking Scheme. All personal health information, i.e. any information relating to the health and well-being of an identifiable individual, is classed as "*confidential*". However, the requirements for the handling and storage of

information classified as *confidential* by the NHS is identical to the requirements for *restricted* information identified in the GPMS. This means that all NHS *confidential* material;

- 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 secure email only.
- 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

5.9 Data Sharing Agreements

There are three levels of documentation which relate to data sharing. These are;

- The **Information Sharing Policy**, a high level agreement to share information between services and agencies within the Highland Data Sharing Partnership.
- These **Information Sharing Procedures** which provide overarching guidance on data sharing for practitioners within the Highland Data Sharing Partnership.
- **Data Sharing Agreements** which define individual instances of data sharing.

Data Sharing Agreements are created to provide guidance and clarification in circumstances where operational processes give rise to a need for planned and recurring data sharing. These agreements describe the **purpose** of data sharing and detail **what** will be shared and with **whom**. Where appropriate agreements also describe **how** data will be shared.

Appendix C to this document provides a blank template for the creation of a Data Sharing Agreement. If you are involved in a process which involves recurring instances of data sharing and you believe that that the creation of a Data Sharing Agreement would be helpful, you should raise this in the first instance with your line manager.

When you are considering sharing data, the first step should always be to check whether a Data Sharing Agreement exists which relates to the purpose for which you are sharing. Where a relevant Data Sharing Agreements exists, this should be followed.

A list of all current Data Sharing Agreements should be maintained by each partner agency. This list should be accessible to practitioners.

6 Resolving Disputes

6.1 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.

6.2 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 or with the person named in the data sharing agreement (see Appendix C). 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 resolve matters. If no resolution is possible, the issue may be escalated to the Highland Data Sharing Partnership.

Details of disputes resolved without escalation to the Highland Data Sharing Partnership must be passed to the Chair of the Highland Data Sharing Partnership. All identifiable personal data must be removed and these should be passed on in the form of statistical reports. 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.

7 Summary

When to share

- Only share when this will lead to improved service provision.
- If sharing to prevent harm and/or to prevent or detect crime, consent is not required.
- Consent must offer a real choice and must be informed and recorded.

What to share

- Only share what is proportionate and relevant to the objectives of the particular instance of data sharing.
- Security of shared data remains the responsibility of the originating agency.
- Shared data may not be shared further without the permission of the originating agency.
- Shared data should not be retained longer than necessary.

Who to share with

- Only share with people who have an identified need-to-know.
- Even when consent is given, the practitioner is responsible for deciding what it is appropriate to share and with whom.
- Keep brief records of data sharing.

How to share

- Make sure you can't be overheard if sharing verbally.
- Only use secure e-mail.
- Only use fax when there is no alternative and take precautions to ensure that only the intended recipient receives the information.
- Portable devices used to store personal data must be encrypted.
- Report immediately the loss of theft of any portable device which contains personal information.

Appendix A Sample Consent Form

MULTI-AGENCY CONSENT FORM

To provide services it may be necessary for professionals and 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 example 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 B Example 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
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

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 abut 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
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

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 caring for you 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 or carers 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

The Highland Council
Comhairle na Gaidhealtachd
SERVING The Highland Community

Northern Constabulary

NHS Highland

Appendix C Data Sharing Agreement Template

AGREEMENT FOR SHARING DATA
BETWEEN ORGANISATIONS

Contact Details

This section should include all the demographic details for the individuals/ departments of all organisations involved in this agreement.

Purpose

This section should explain why this Data Sharing Agreement is necessary and describe the aims and benefits associated with it.

Basis for Sharing

This section should describe the legal basis for sharing under this agreement. If this is based on consent, this section should describe what happens if consent is withheld or withdrawn. If sharing is based on a particular statutory power or covers only the sharing of anonymised or statistical information, details should be provided.

Details of Information to be Shared

This section should detail

- What information is to be shared
- Why it is to be shared
- When sharing is to commence
- How it is to be shared i.e. phone, email, case-conferences
- Is client consent necessary – explain if not
- Has client consent been obtained
- Has client consent been overridden – explain why
- What level of control should be marked on the information

Handling the Information

Transmission

Client identifiable or sensitive information must be secured in a double envelope with the protective marking shown on the inner one only.

When transmitting information via other methods e.g. email, fax or telephone, this must be done as per the policies and procedures of each organisation.

Storage

All information must be kept securely when not in the personal custody of an authorised person. The 'need-to-know' principle will be applied. Client identifiable or sensitive information must be stored as per the policies and procedures of each organisation.

Release to Third Parties

No information exchanged by the partners to this procedure will be released to any third party without the permission of the originating partner. This includes Subject Access and FOI(S)A requests.

Resolving disputes

This section should include contact details for one person in each participating agency to whom disputes should be escalated if they cannot be resolved by practitioners/line managers.

Review

This section should describe how and when the ongoing effectiveness of this agreement will be reviewed.

DESCRIPTION OF TYPE OF INFORMATION WHICH IS TO BE SHARED AND BETWEEN NAMED ORGANISTATIONS

EXAMPLE:

INFORMATION ON 'XXXXXXXXXX'
BETWEEN
NHS HIGHLAND
NORTHERN CONSTABULARY
HIGHLAND LOCAL AUTHORITY

CONTACT DETAILS

EXAMPLE:
(Information Sharing Organisation 1)
Main Contact
Job Title
Department
Location
Phone Number
Mobile Phone Number
Email Address
Fax Number

(Information Sharing Organisation 2)
Main Contact
Job Title
Department
Location
Phone Number
Mobile Phone Number
Email Address
Fax Number

(Information Sharing Organisation 3)
Main Contact
Job Title
Department

DETAILS OF INFORMATION TO BE SHARED

EXAMPLE:

When, What, Who, How

Consent Required and reasons

What level of control