Scottish Accord on Sharing Personal Information

1 Introduction and Purpose

1.1 Introduction

1.1.1 The Scottish Accord on the Sharing of Personal Information (SASPI) is based upon the Wales Accord on the Sharing of Personal Information (WASPI), which was endorsed by the Welsh Assembly Government as the 'single' information sharing framework for Wales, and has been widely utilised. Based on this positive experience, the Scottish Government has adapted and adopted the WASPI documentation for use across Scotland.

1.1.2 The purpose of the framework is to enable service-providing organisations directly concerned with the safeguarding, welfare and protection of the wider public to share personal information between them in a lawful and intelligent way.

1.1.3 The SASPI framework supports the drive to share personal information on individuals; legally, safely and with confidence. It aims to support the public in receiving services that are coherently and collaboratively delivered and effectively based on need, and safeguard the information rights of the individual.

1.1.4 Adoption of the framework across Scotland will help ensure compliance with statutory and legislative requirements for disclosing person identifiable information including the Data Protection Act 1998, the Human Rights Act 1998, the common law duty of confidentiality, and relevant professional codes of conduct. It also enables compliance with the Information Commissioner's Data Sharing Code of Practice.

1.1.5 The Information Commissioner's Office within Wales welcomed the implementation and use of the WASPI framework stating that "WASPI seeks to facilitate lawful exchange of information between organisations by establishing and setting out practical mechanisms for this exchange, and it is likely to lead to increased levels of confidence and compliance".

1.1.6 This framework applies to all public sector organisations, voluntary sector organisations and those private organisations contracted to deliver relevant services to the public sector and who provide services involving the health, education, safety, crime prevention and social well being of people in Scotland. In particular, it concerns those organisations that hold information about individuals and who may consider it appropriate or necessary to share that information with others.

1.1.7 The conditions, obligations and requirements set out in this Accord, and Protocols developed in support of it, will apply to all appropriate staff, agency workers, volunteers and other data processors working on behalf of the partner organisations including agents and sub-contractors.

1.1.8 Organisations providing services to individuals or Service Users[1] within Scotland will need to process information about them. Often the information which is processed constitutes "personal information." For the purposes of this Accord personal information is information which relates to an individual, including their image or voice, which enables them to be uniquely identified from that information on its own or from that and / or other information available to the organisation (see glossary for full definition).

1.1.9 At times, more than one organisation may become involved in the provision of a service to an individual. This may require that relevant, minimum and appropriate personal information be shared between them and their Practitioners, in order that each can deliver co-ordinated, effective and seamless services to the Service Users involved.

1.2 Approach

1.2.1 To ensure that Service Users receive the 'seamless', high quality support or service relevant to their needs a co-ordinated, multi-agency approach may be appropriate. It may then be necessary for those involved to share personal information between the organisations and this requires both mutual trust and confidence in the way that each manages that information.

1.2.2 Each organisation will acknowledge the need to comply with the requirements of codes of practice within their field of expertise and to take account of appropriate guidelines relevant to their field of work.

Example: Code of Practice

Participating health organisations will acknowledge the need to comply with the requirements of the NHSScotland *Code of Practice on Protecting Patient Confidentiality*.

This document provides:

- generic guidance and advice on the requirements of providing a confidential service;
- generic advice on the disclosure of personal information;
- specific guidance for health care professionals.

1.3 The Framework for Sharing Personal Information

1.3.1 The framework consists of two elements: (a) this Scottish Accord on the

[1] Service Users is intended as an inclusive term to describe those people who have contact with service providing organisations within Scotland

Sharing of Personal Information and (b) Information Sharing Protocols developed within this framework.

(a) The Scottish Accord on the Sharing of Personal Information (SASPI)

The Accord identifies the commitments required by each organisation to enable sharing of personal information. Sign up and ownership is at the highest level.

1. It is a statement of the principles and assurances which govern the activity of information sharing. It ensures that the rights of all those who are involved in the process are protected.

(b) Information Sharing Protocol (ISP)

An ISP focuses on the purposes underlying the sharing of specific sets of information. It is intended for operational management and staff and provides the details of the processes for sharing information, the specific purposes served, the people it impacts upon, the relevant legislative powers, what data is to be shared, the consent processes involved, any required operational procedures and the process for review.

The ISP communicates to Practitioners the operational requirements, setting out the who, what, why, where, when, and how of sharing information.

Supporting Documentation

A range of guidance documents, templates and approved ISPs have been developed to assist partner organisations in implementing the framework and are available on the SASPI website. Further assistance regarding development of an ISP can be sought from the eHealth Information Assurance Team.

1.3.2 All signatory organisations must demonstrate that, in adopting the agreed standards and good practice, they will meet or exceed the principles set out in this Accord.

1.4 Information Excluded from the SASPI Framework

1.4.1 There are two broad categories of information relating to Service Users that organisations may share without the need for an Information Sharing Protocol:

Aggregated (Statistical) Information

Aggregated and management information is used to plan and monitor progress of the organisation in its delivery of services. This is generally outside the scope of the Data Protection Act 1998 on the basis that a living individual could not be identified from such data.

Depersonalised and Anonymised Information

Information that has had all personal information removed so as to render it anonymous and therefore outside the scope of the Data Protection Act 1998.

Care must be taken, with all aggregated, depersonalised and anonymised information, where it may still be possible to identify individuals e.g. in areas of low population density / low occurrence.

1.5 Adoption of the Accord

1.5.1 Formal adoption of the Accord is the responsibility of the Chief Executive or Chief Officer of either a statutory body or a private or voluntary sector organisation.

1.5.2 Each signatory organisation agrees to support the adoption, dissemination, implementation, monitoring and review of this Accord and its requirements in accordance with its own internal and any other jointly agreed and authorised information governance standard and / or operational policies and procedures.

1.5.3 To facilitate this, each organisation will identify a “Designated Role” who will have this responsibility.

1.5.4 The signatory form ‘Declaration of Acceptance and Participation’ is available on the Knowledge Network website, in the SASPI section, at: <insert URL>

2 Organisation Commitments

2.1 Introduction

2.1.1 This section outlines the principal commitments that each signatory organisation will make. When fully implemented these should ensure that the organisation's treatment of Service Users' information is compliant with current legislation and good practice. There is a 'Self Assessment Checklist' available on the website for organisations to use if they wish to assess their current position. It may also be used as a review document.

2.2 Service Users

2.2.1 Each organisation must inform Service Users that information is being collected and recorded about them, the reasons or purposes for doing so (including any statistical or analytical purposes), the persons or organisations with whom it may be shared and the reasons for such sharing. This is known as a 'Fair Processing or Privacy Notice'.

2.2.2 Each organisation must also inform Service Users about their rights, in respect of legislation and how these may be exercised. This will include the provision of appropriate support in order that Service Users may best exercise those rights e.g. providing information in alternative formats or languages, providing support in the form of advocacy or assisting them to make a subject access request under Section 7 of the Data Protection Act 1998.

2.2.3 Service Users generally have the right to object to the use and disclosure of certain personal information and need to be made aware of this right by participating organisations. It should not be assumed that Service Users are content for their personal information to be used for purposes other than those directly associated with their receipt of services from the organisation to which they provided their information.

2.2.4 All Service Users have the right to expect that information disclosed by them or by other parties about them to an organisation will be protected, managed and processed with the appropriate degree of privacy and confidence. However, Service Users' rights to prevent disclosure of their personal information may be overridden in certain circumstances in accordance with legislation and common law.

2.2.5 Each organisation must ensure that they have appropriate policies and procedures in place to facilitate both the protection and the exercising of these and other rights. Each organisation will comply with the rights of the Service User in a fair and consistent manner and in accordance with any specific legislative requirements, regulations or guidance.

2.3 Consent

2.3.1 If a patient has been informed what information is to be disclosed, the purpose and the extent of disclosure, and that they have the right to object but have not objected, then this is sufficient and explicit consent is not required. For example, service users who agree to receive health and social care services from an organisation should be made aware that data sharing between agencies may be required to enable effective service provision. In specific circumstances, where data sharing would be controversial or unexpected by the Service User, additional informed consent is required. When consent is collected the Service user should understand what personal information is recorded and why, what future use will be made of it and the length of time it is likely to be retained. The Service Users should also have explained to them the possible consequences of refusing or withdrawing consent and the exceptional circumstances in which a decision may be taken to share without consent.

2.3.2 Other than in exceptional circumstances, Service Users have the right to object to information they provide in confidence being disclosed to others in a form that identifies them, even where the latter are providing essential care or services.

2.3.3 Service Users will be informed that they are entitled to limit the disclosure of their information in accordance with their preferences, except where exceptional circumstances apply.

2.3.4 If consent is required to enable the collection or disclosure of information, it has to be informed, fair and specific for the purposes for which it was obtained. Procedures for obtaining consent within the law will be agreed between partner organisations and detailed in the Information Sharing Protocols.

ISPs should mention that when obtaining consent, the Service Users must be informed of the purposes for which the information is being collected, how it will be used and with whom it will be shared.

2.3.5 Information Sharing Protocols should include procedures for:

- Obtaining consent;
- Establishing fitness to give consent; and,
- Recording consent.

2.3.6 Information may only be shared without consent in circumstances where it is justified and compatible with the requirements of current legislation, or there is a public interest in disclosing information to protect individuals or society from risks of serious harm such as:

- Serious crime;
- Serious communicable diseases;
- Child Protection – where it is judged that a child or young person is at risk of significant harm; or
- Adult Protection - where it is judged that a vulnerable adult is at risk of

significant harm.

When considering whether the disclosure is justified in the public interest, you must be satisfied that person-identifiable information is necessary for the purpose or it is not reasonably practicable to anonymised.

2.3.7 The Data Protection Act authorises disclosure where this is necessary for medical purposes without requiring explicit consent, although the Code of Practice on Protecting Patient Confidentiality should still be complied with.

2.3.8 Reasons that lead to a decision to proceed with a disclosure without consent must be fully documented and, where appropriate, be filed in the Service User's record. Wherever practical and possible participating organisations must inform the Service User of the decision and the reasons for it and indicate the legal basis on which the disclosure is permitted or required.

Please note: Staff should not hesitate to share personal information in order to prevent abuse or serious harm, in an emergency or in life-or-death situations. If there are concerns relating to child or adult protection issues, the relevant organisational procedures must be followed.

2.3.9 Each participating organisation will have in place and apply an appropriate decision making process which is compliant with the Adults with Incapacity (Scotland) Act 2000.

2.3.10 The following principles must be applied when deciding whether a measure under the Act is necessary and if so, which will be the most appropriate to meeting the needs of the individual. The principles must also be applied by anyone appointed with powers under the Act when a decision needs to be taken on behalf of the individual. It is also recognised good practice that the principles should be applied in relation to all decision-making for a person with impaired decision-making capacity, regardless of whether he/she has a proxy under the Act.

Principle 1 - benefit

- any action or decision taken must benefit the adult and only be taken when that benefit cannot reasonably be achieved without it.

Principle 2 - least restrictive

- any action or decision taken should be the option that restricts the person's freedom as little as possible but at the same time enables the purpose of the action to be achieved.

Principle 3 - take account of the past and present wishes and feelings of the adult

- In deciding if an action or decision is to be made, and what that should be, account shall be taken of the present and past wishes and feelings of the adult, as far as they can be ascertained. The person should be offered appropriate assistance to communicate their views (for further guidance see Appendix 1 of guidance on the Adults with Incapacity (Scotland) Act 2000).

  Note: that it is compulsory to take account of the present and past wishes and feelings of the adult if these can be ascertained by any means whatsoever.

Principle 4 - consultation with relevant others

- In deciding if an action or decision is to be made and what that should be, account shall be taken of the views of: the nearest relative and the primary carer of the adult; the adult's named person; any guardian or attorney with powers relating to the proposed intervention; any person whom the Sheriff has directed should be consulted; any other person appearing to have an interest in the welfare of the adult or the proposed action, where these views have been made known to the person responsible - in so far as it is reasonable and practicable to do so.

Principle 5 - encourage the adult to exercise whatever skills he or she has and to develop new skills as far as possible.

2.3.12 Normally personal information about children **will not** be shared without the informed consent of the child himself or herself or a person with parental responsibility. Further guidance relating to sharing information relating to children will be contained in individual ISPs including links to the Age of Legal Capacity (Scotland) Act 1991 and the Children (Scotland) Act 1995.

2.3.13 Individual ISPs will provide further guidance on the conditions which must be met before information can be shared and the circumstances in which information can be shared without consent.

2.4 Staff and Others with Access to Information

2.4.1 Each organisation must have in place internal operational policies and procedures that will facilitate the effective processing of personal information which is relevant to the needs of the organisation, its Managers, Practitioners and Service Users.

2.4.2 Staff contracts must contain appropriate confidentiality clauses that detail possible consequences of unauthorised or inappropriate disclosure of Service User information.

2.4.3 Each organisation must ensure that all staff have the necessary level of Disclosure Scotland clearance.

2.4.4 Each organisation must ensure that all relevant staff receive training,

advice and ongoing support in order to be made aware, and understand the implications, of:

- this Accord and any associated documentation. This should include any associated operational requirements arising from their implementation;
- the law which applies generally and in relation to the performance of the specific statutory powers and functions of the participating organisation concerned;
- the Data Protection Act, the Human Rights Act and the common law duty of confidentiality;
- Relevant Codes of Practice and any other associated regulations and guidance.

2.4.5 Each organisation must have in place disciplinary procedures which will be invoked if a member of staff is found to have breached the confidentiality of a Service User or to have shared information in a manner in contravention of this Accord.

2.4.6 Where a partner organisation relies on a third party to process personal information the organisation must have in place appropriate contractual data processing and confidentiality agreements.

2.5 Designated Role

2.5.1 Each organisation must identify a "Designated Role(s)" who will have responsibility for implementing and monitoring their commitments under this Accord.

2.6 Data Protection Act Notification

2.6.1 Each organisation must have an appropriate entry (Notification) in the "Register of Data Controllers" managed by the Information Commissioner's Office. It is the responsibility of each organisation to ensure that its entry is kept accurate and up-to-date.

2.7 Dissemination

2.7.1 Participant public organisations will place this Accord and other framework documentation on its Freedom of Information (Scotland) Act 2002 Publication Scheme so that it is proactively published in accordance with the terms of the Freedom of Information (Scotland) Act. Where partner organisations are not bound by this legislation then consideration should still be given to placing this information on their website where available.

2.8 Information Retention

2.8.1 All participating organisations will have a policy document which will make clear their approach to retention, storage and disposal of records, to the standards of the Public Records (Scotland) Act 2011.

2.9 Quality and Accuracy of Personal Data

2.9.1 Each organisation is responsible for the quality and accuracy of the personal information it obtains, records, holds, uses and shares.

2.9.2 If it is discovered that information held is inaccurate, partner organisations must ensure that their records / case management systems are corrected or updated accordingly. The organisation will take reasonable steps to advise any other party known to have received or to be holding that information about any change which it is necessary to make.

2.10 Information Security

2.10.1 Each organisation must have in place a level of security commensurate with the sensitivity and classification of the information to be stored and shared.

2.10.2 Each organisation must ensure that mechanisms are in place to address the issues of physical security, security awareness and training, security management, systems development, role based security / practitioner access levels, receiving and transfer of data and system specific security policies. The standard applied should be ISO 27001.

2.10.3 Each organisation must consider the impact on individuals' privacy and undertake an appropriate Privacy Impact Assessment before developing any new IT system or changing the way they handle personal information.

2.10.4 It is accepted that each organisation will vary in size and complexity and this will be reflected in any processes and levels of security put into place.

2.11 Evaluation and Research

2.11.1 Each organisation may use personal information for the purpose of evaluation and research, jointly or independently, including the use of agents acting on the organisation's behalf, provided that:

- the purpose is contained within the organisation's notification to the Information Commissioner's Office;
- correct procedures for research are adhered to i.e. relevant research and ethics committees;
- Service Users have been informed of this purpose and have provided consent when appropriate, in accordance with Data Protection Act 1998 provisions on research;
- information is anonymised and / or aggregated whenever possible;

- data processing agreements are in place where required by law.

2.11.2 Where a proposed research subject lacks capacity to decide whether to participate in research, the Adults with Incapacity (Scotland) Act 2000 part 5 will apply.

2.12 Marketing and Commercial Purposes

2.12.1 Partner organisations must not use personal information that has been shared between them for the purpose of any marketing and / or commercial activities unless:

- processing for marketing and commercial purposes is listed within the notification to the Information Commissioner's Office of both the organisation that collected the information and any organisation using the information for marketing and / or commercial activities;

and

- Service Users have been informed of this purpose and provided explicit consent.

2.13 Professional Ethic and Codes of Conduct

2.13.1 Staff will adhere to their professional codes of conduct and / or practice in respect of information given in confidence. However, compliance with any relevant professional code does not authorise the sharing of information where such sharing is not also permitted by law.

2.13.2 Partner organisations will recognise that individual professionals are accountable to their professional regulatory body in complying with their respective codes of conduct and each organisation will take into account these requirements before reaching any decision to share information accordingly.

3 Monitoring of the Framework

3.1 Introduction

3.1.1 This section outlines the reporting arrangements that each partner organisation must have in place to monitor non-compliance with the SASPI framework.

3.2 Non-compliance (Internal)

3.2.1 Instances of internal non-compliance with this framework and associated procedures will be logged and reported to the appropriate Designated Person. Each incident will be dealt with promptly in accordance with the agreed information governance / operational policies and procedures.

3.3 Non-compliance (Partner Organisations)

3.3.1 Instances of non-compliance with this framework and associated procedures by a partner organisation will be reported to each of the organisation's Designated Persons. Each incident will be dealt with promptly in accordance with agreed information governance / operational policies and procedures. Where appropriate, a meeting of each partner organisation's Designated Person(s) may be established to investigate such incidents and agree outcomes.

3.3.2 In addition, where non-compliance is likely to amount to professional misconduct as defined by an appropriate regulatory body; then it is expected that it will be reported to that regulatory body by the Designated Person of the partner organisation concerned.

3.3.3 Any contracts or service level agreements between partner organisations must make provision for dealing with incidents of non-compliance in line with this framework.

3.4 Service Users / Practitioners' Concerns and Complaints

3.4.1 Any concerns or complaints received from Service Users relating to the processing / sharing of their personal information will be dealt with promptly and in accordance with the internal complaints procedures of that partner organisation and, where appropriate, may be raised with other partner organisation's Designated Persons.

3.4.2 Any similar concerns or complaints received from Practitioners relating to the sharing of information under the framework will be referred to their organisation's Designated Person, who will respond in accordance with the internal policies and procedures of that organisation. Again, where appropriate, it may be raised with other partner organisation's Designated Persons.

3.5 Formal Review

3.5.1 This Accord will be reviewed every four years or as legislation dictates, by the appropriate national review group.

3.5.2 ISPs are subject to local review by partner organisations and should be conducted at least every 2 years.