
Information Sharing Protocol

Version Number:

7.0 Final

Prepared By:

Information Governance

Effective From:

March 2009

Review Date:

March 2010

Ratification Process:

East Ayrshire Council

North Ayrshire Council

South Ayrshire Council

NHS Ayrshire & Arran

VERSION CONTROL

The Ayrshire Information Sharing Protocol will be reviewed on an annual basis.

Details of distribution, additions or changes to the ISP are as follows:

Revision Date	Version	Responsible Officer	Summary of Changes
June 2004	V3		Version 3 released following local review and update for IAF.
Sept 2005	V4 Draft		Updated following Scottish Executive review and feedback against eCare Gold Standard ISP
Sept 2008	V5 Draft	NHS A&A Information Governance Manager	Section on Subject Access Requests added comments from 3 Local Authorities and NHS A&A incorporated
			EAC comments - technical
Oct 2008	V6 draft		IG Update
Dec 2008	V7 draft		IG Update
Mar 2009	V7.0 Final		Ratified by Data Sharing Partnership Steering Group

AGENCY ISP GATEKEEPERS

NHS Ayrshire & Arran will take responsibility for the overall control, update and distribution of the Ayrshire Information Sharing Protocol via the gatekeepers named below.

The following organisations are responsible for the distribution of the Ayrshire Information Sharing Protocol and ensuring that the latest version of the ISP and associated guidance are in use:

East Ayrshire Council
South Ayrshire Council
North Ayrshire Council
NHS Ayrshire and Arran

Table of Contents

<u>1. Statement & Introduction</u>	4
<u>2. Scope</u>	5
<u>3. Objectives</u>	5
<u>4. Defined Purposes</u>	6
<u>5. General Principles</u>	6
<u>6. Access and Security</u>	10
<u>7. Responsibility for Management of Protocol</u>	11
<u>8. Relevant Documentation</u>	12
<u>9. APPENDIX 1</u>	13
<u>10. APPENDIX 2</u>	14

1. Statement & Introduction

- 1.1 Information sharing between the Ayrshire partner agencies is vital to the provision of co-ordinated and seamless health and social care services. This protocol exists to ensure that information can be shared in a way which satisfies the legal and professional obligations of the parties involved, their respective staff, and the legitimate expectations of service users. It is not intended to be used as an operational guide book or manual, instead, it simply defines at a high level, general agreed principles for information sharing between the parties.
- 1.2 Each individual context of information sharing (e.g. Community Care, Children & Families) will require a unique set of Guidance Procedures that should be used in conjunction with this protocol.
- 1.3 The aim of public policy is that individuals receive the services that they need and that the organisation of services should not impede or debase the service provided. This clearly requires agencies to work effectively and efficiently together to tailor services to the particular circumstances of each individual.
- 1.4 This protocol is designed to ensure that the exchange of information which is necessary to permit multi-agency and multi-disciplinary service can proceed in a way which conforms with all applicable laws and safeguards the rights of the parties and service users.
- 1.5 Any sharing of confidential details about individuals must be controlled, transparent and compliant with relevant legal and ethical requirements. To safeguard the information that is shared, appropriate security measures will need to be put in place.
- 1.6 The agencies acknowledge that under certain circumstances there will be a need to disclose personal identifiable information to each other to ensure on-going co-ordinated and seamless health and social care services are not compromised. This document outlines the terms and conditions agreed between the agencies under which personal identifiable information will be shared and the safeguards that must be implemented.
- 1.7 Staff within NHS Ayrshire & Arran must adhere to the Caldicott Principles and the NHS Scotland Code of Practice on Protecting Patient Confidentiality which state that patient identifiable information may only be shared on a strict 'need to know' basis.
- 1.8 In order to ensure individuals receive quality services, it is vital that information be shared and that staff involved have ready access to the information they need. Individual service users and their carers must have implicit trust that their personal identifiable information will be kept secure and confidential and that their privacy is respected at all times.
- 1.9 There will be one nominated Senior Professional Officer within each agency who will be responsible for agreeing the protocol and any subsequent amendments. All proposed amendments must be made in writing and signed by the agreed nominated Senior Professional Officer(s). No amendments will otherwise be accepted.

- 1.9 Personal identifiable information will be transferred between the agencies in compliance with each agencies own secure transportation of personal data policy and procedures and the terms of this protocol. Each agency must maintain up-to-date registers of personnel and access rights for personal information. Staff within agencies will be assumed to have access rights in accordance with their own strict need to know principles or codes (see 1.7).

2. Scope

- 2.1 This protocol covers personal identifiable information, held in both manual and electronic format and is collected in order that individuals may receive quality services from the agencies below:

NHS

- NHS Ayrshire & Arran

Local Authorities:

- South Ayrshire Council
- East Ayrshire Council
- North Ayrshire Council

3. Objectives

The objectives of this Protocol document are to:

- 3.1 Set parameters for the sharing of information between Ayrshire partner agencies.
- 3.2 Define justified purposes for sharing personal identifiable information between Ayrshire partner agencies.
- 3.3 Define the requirement to obtain, record and check for valid informed consent for the sharing of personal identifiable information between Ayrshire partner agencies.
- 3.4 Define circumstances where personal identifiable information can be disclosed without consent.
- 3.5 Define requirements to keep personal identifiable information secure and limit access on a strict need to know basis.
- 3.6 Define requirements for processing subject access requests.

4. Defined Purposes

4.1 The following are purposes agreed as justifiable for the transfer of personal identifiable information between agencies, as defined within the remit of this protocol. It should be noted however that the list is not exhaustive. All staff are reminded that only **relevant** personal identifiable information should be shared on a 'need to know' basis and that they have a responsibility to make themselves aware of the circumstances of each individual situation:

- Delivery of integrated services
- Assuring and improving the quality of services
- Monitoring, reporting and protecting public health
- Managing and planning future services*
- Contracting for services*
- Auditing accounts and performance
- Statutory obligation
- Risk management
- Court orders
- Research/trials*
- Statistical analysis*
- Investigation of complaints or potential legal claims*
- Medical reports/insurance requests*
- Child Protection

if **personal identifiable information is shared for the purposes marked with an asterisk above, the consent of the individual must be obtained. This consent may be implied or explicit dependent upon local operational procedures. (See Section 5.2 Consent & Disclosure).*

5. General Principles

5.1 Key Legislation

5.1.1 Anyone working for the agencies that are part of this agreed protocol has an obligation to safeguard the confidentiality of personal information. This is governed by law; Data Protection Act 1998, the Common Law Duty of Confidentiality, Human Rights Act, as well as individual contracts of employment, organisational obligations and also by professional codes of conduct.

5.1.2 The DPA 1998 requires that the processing of personal data complies with the following eight Data Protection Principles:

- Personal data must be processed fairly and lawfully.
- Personal data shall be obtained for only one or more lawful purpose and must not be further processed for incompatible purposes.
- Personal data shall be adequate, relevant, and not excessive.
- Personal data shall be accurate, and where necessary, kept up to date.

- Personal data shall not be kept for longer than necessary.
- Personal data shall be processed in accordance with the rights of data subjects under the Act.
- Appropriate technical and organisational measures shall be taken to prevent unauthorised or unlawful processing of data and against accidental loss or destruction of, or damage to data.
- Personal data shall not be transferred to a country outside the European Economic Area, unless that country ensures an adequate level of protection for the rights and freedom of individuals in relation to processing the data.

5.1.3 Each individual has six rights in respect of their own personal data held by others.

- the right of subject access
- the right to prevent processing likely to cause damage or distress
- the right to prevent processing for the purposes of direct marketing
- the rights in relation to automated decision taking
- the right to take action for compensation if the individual suffers damage
- the right to take action to rectify, block, erase or destroy inaccurate data

Data subjects also have the entitlement to make a request to the Information Commissioner for an assessment to be made as to whether any provision of the DPA 1998 has been contravened.

5.1.4 Personal identifiable information falls into two separate categories; 'personal information' and 'sensitive personal information'. In order for processing of personal data to be lawful, at least one of the conditions listed in schedule 2 of the DPA 1998 must be met and if processing 'sensitive personal data', at least one additional condition from Schedule 3 must be met. Schedules 2 and 3 to the DPA 1998 are set out in Appendices 1 and 2.

5.1.5 Health records about a person's physical or mental condition are classed as 'sensitive personal information' under the Act. Only under exceptional circumstances will personal identifiable information be disclosed out-with the originating organisation without the patient's consent. One example of when this might occur would be when the personal identifiable information is required by statute. For the full list of these 'exemptions' see Part IV of the Data Protection Act 1998.

5.1.6 Where it is judged that an individual is unable to provide consent (for example due to mental incapacity or unconsciousness), conditions in Schedule 2 and 3 of the DPA 1998 still must be satisfied (processing will normally need to be in the vital interests of the individual) unless there is someone else who is lawfully entitled to consent on behalf of the individual and who does, in fact, consent. Any such proxy consents should be in writing for the avoidance of any later disagreement.

5.1.7 In accordance with the requirements of the Common Law Duty of Confidentiality, if information is given in circumstances where it is expected that a duty of confidence applies, that information cannot normally be disclosed without the data subject's

consent. Total confidentiality is expected unless there is a compelling reason why it should not; examples of these are already mentioned in 5.1.6.

- 5.1.8 Article 8.1 of the European Convention on Human Rights, as given effect to by the Human Rights Act 1998, provides that “everyone has the right to respect for his private and family life, his home and his correspondence.” This is however, a qualified right i.e. there are specified grounds upon which it may be legitimate for authorities to infringe or limit those rights and Article 8.2 provides “there shall be no interference by a public authority with the exercise of this right except 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.”
- 5.1.9 The Freedom of Information (Scotland) Act 2002 (herein referred to as FOISA) provides a statutory right of access to all information held by Scottish public authorities, unless one of the exemptions to this right of access is applicable. Public authorities will require procedures in place to facilitate disclosure of information under this legislation. One of the exemptions in the FOISA relates to personal information, and requires that any disclosure of personal data to a third party must comply with the data protection principles contained in the DPA 1998.
- 5.1.10 Each employing agency has a statutory duty to manage the risk to safety of their own staff and to exercise a duty of care towards persons not in their own employment, therefore it is essential to consider the implications of non-compliance with the Health & Safety at Work Act 1974 in conjunction with requirements of the DPA 1998 and the Common Law Duty of Confidentiality.

Consent & Disclosure

- 5.2.1 Implied consent is where the individual, having been given information about the disclosure and the opportunity to express objection accepts a service without voicing an objection.
- 5.2.2 Within individual agencies, implied consent may be acceptable in circumstances where an individual will be a participant in the process and would expect personal identifiable information to be recorded and seen by those involved in providing the care within that agency.
- 5.2.3 Explicit consent is where an individual actively expresses consent orally or in writing.
- 5.2.4 Any member of staff, who may have to seek the consent of an individual to share personal identifiable information about them must understand and be able to explain or provide clearly the purpose and implications of sharing information, what this may entail, and the safeguards of confidentiality that apply.
- 5.2.5 Consent will be sought at the earliest opportunity and at the very least prior to person identifiable information being shared with any other agency.

- 5.2.6 When sharing information explicit consent should be sought whenever possible. However, it may not be practical, or necessary to seek an individual's explicit consent each time that personal identifiable information needs to be shared for the defined purposes. (See Section 4 – Defined Purposes). Regardless of the situation however, individuals must always be fully informed of the uses to which their information may be put. All agencies must ensure that this requirement is met.
- 5.2.7 Exceptional circumstances in which an individual's consent may be overridden would include where information is required by statute (e.g. Abortion Regulations 1991, Road Traffic Act 1988, Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1985, Mental Health (Care and Treatment)(Scotland) Act 2003) or court order, where there is serious risk to public health, risk of harm to other individuals or for the prevention, detection or prosecution of serious crime. Where there is the potential for harm to children or where children have already been identified as being at risk through child protection procedures, then the need for consent is overridden and information should be shared with appropriate agencies.
- 5.2.8 Anonymised information, which is information stripped of all personal identifiers, is another situation where information may be shared to support legitimate activity without the consent of the individual. Examples of this are for research and statistical or planning purposes. However, here again it should be noted that even when personal identifiable information has been successfully anonymised, individuals must still be informed of the proposed use(s) of this anonymised information. Staff, are encouraged to use anonymised data wherever practicable to safeguard privacy and confidentiality.
- 5.2.9 Requests for access to personal identifiable information for purposes other than those defined must be submitted to the nominated Senior Professional Officers for consideration and subsequent approval or rejection. Where approval is given proof of consent will be required prior to any personal identifiable information being transferred.
- 5.2.10 Where a person does not have the capacity to make an informed decision but a third party has authority to act as their guardian and take decisions on their behalf, then the information sharing protocol and all that is included in it must be explained to that third party in the same manner that it would initially have been explained to the individual.
- 5.2.11 In the absence of a legal or welfare guardian – see Part 6 of the Adults with Incapacity (Scotland) Act 2000 - the decision should be made on the individual's behalf by those responsible for providing care, taking into account all known views, with the individual's best interests being paramount. The reasons for the final decision must be clearly documented and signed by the appropriate nominated Senior Professional Officer(s).

- 5.2.12 The agencies recognise that for the purposes of the rights affected by this protocol, as defined in the Age of Legal Capacity (Scotland) Act 1991 individuals of or over the age of 12 are presumed to have full capacity to take decisions in their own right. Accordingly, any disclosure of information relating to a young person with the requisite mental capacity, made to their parent or guardian without the consent of the young person, will need to be justified in the same way as any other disclosure of personal identifiable information without consent.
- 5.2.13 Procedures will be put in place to ensure that any decision to disclose personal identifiable information without consent has been fully considered in terms of applicable legislation. This will often require the relevant staff to make difficult professional judgments about what level of information sharing, if any, is necessary to protect the vital interests of the individual or the public. Any risk assessment should show that staff members have taken all relevant factors into consideration before reaching a decision. Any decision made about the sharing of personal identifiable information without consent should be proportionate. This means that the overall benefit achieved by the decision should outweigh any interference with the rights of an individual.
- 5.2.14 Partner agencies must ensure that shared information which is to be released without consent has the approval of the other agency or agencies who share the same information.
- 5.2.15 If personal identifiable information is disclosed without consent, then a full description of the information disclosed will be recorded, the reasons why the decision to disclose was taken, the person who authorised the disclosure and the person(s) to whom it was disclosed.
- 5.2.16 Each agency will have an on-call executive officer who has the authority and knowledge to take responsibility for decisions taken to share information without consent. This authority will be available out-with normal working hours to enable emergency situations to be dealt with.
- 5.2.17 To support staff, agencies shall put in place agreed procedures that give clear guidance on obtaining and recording individual informed consent, withdrawal of consent or refusal to give consent.

6. Access and Security

- 6.1 In line with DPA 1998 Principle 7, each agency must take appropriate technical and organisational measures to prevent unauthorised or unlawful processing of personal data and against accidental loss or destruction, or damage to personal data.
- 6.2 As a minimum, to ensure a satisfactory standard of security and restricted access, each agency must have in place up to date policies and procedures to cover the following:

Information Security
Secure transportation of personal data
Buildings Security
Secure storage, retention and destruction of records.
Acceptable Use of Internet and E-Mail.
Data Protection
Freedom of Information
Subject Access

- 6.3 In line with the DPA 1998, every organisation (data controller) that processes personal data in an automated form must notify the Information Commissioner of the purposes they process personal data, unless they are exempt. All agencies must ensure they comply with this requirement and maintain an up-to-date and accurate registration with the Information Commissioner.
- 6.4 In the event of a security breach where the personal identifiable information has been made substantially susceptible to or which has been breached originates from a partner agency, the incident should be reported immediately to the nominated Senior Professional Officer(s) and member(s) of staff within that agency responsible for Data Protection.
- 6.5 A subject access request (see 5.1.3) may be submitted to a partner agency rather than to the organisation where the personal identifiable information originated from i.e. individuals may request access to information that is held by an organisation but did not originate from that organisation.
- 6.6 If the information requested consists of information as to the physical or mental health of the data subject and the data controller is not a health professional (as defined in The Data Protection (Subject Access Modification) (Health) Order 2000 (S.I. No 413)) the information should not be provided unless the appropriate health professional has been consulted. Agencies must draft agreed procedures to handle requests of this nature.

7. Responsibility for Management of Protocol

- 7.1 The nominated Senior Professional Officers (SPO) for each agency are collectively responsible for ensuring the terms of this protocol are adhered to by those staff/agencies to which confidential information is supplied.
- 7.2 Any breaches of the Protocol must be brought to the immediate attention of the nominated SPO for the agency concerned. The SPO concerned will then liaise with other partner agency SPO's involved to agree on any appropriate action or otherwise that may be necessary.
- 7.3 Each organisation should ensure that all staff involved in the sharing of personal identifiable information are given adequate training in all aspects of this protocol and the relevant supporting policies, procedures and documentation.

8. Relevant Documentation

8.1 This Protocol has been drawn up taking into account the following legislation and guidance documents:

- [Human Rights Act 1998](#)
- [Data Protection Act 1998](#)
- [Data Protection \(Subject Access Modification\) \(Health\) Order 2000 \(S.I. No. 413\)\)](#)
- [Freedom of Information \(Scotland\) Act 2002](#)
- [Adults with Incapacity \(Scotland\) Act 2000](#)
- [Age of Legal Capacity \(Scotland\) Act 1991](#)
- [Health and Safety at Work Act 1974](#)
- Common Law Duty of Confidentiality
- [NHS Scotland Code of Practice on Protecting Patient Confidentiality](#)
- NHS Caldicott Principles
- Gold Standard Information Sharing Protocol – Guidance Note
- BS7799 British Standard in Information Security
- [NHS Scotland Information Security Policy and Standards HDL \(2006\) 41](#)
- Mental Health (Care and Treatment)(Scotland) Act 2003

9. APPENDIX 1

DPA 1998

SCHEDULE 2

Conditions relevant for the purposes of the first principle: Processing of personal data

1. The data subject has given his consent to the processing.
2. The processing is necessary-
 - (a) for the performance of a contract to which the data subject is a party, or
 - (b) for the taking of steps 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. (1) 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.

(2) The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.

10. APPENDIX 2

DPA 1998

SCHEDULE 3

Conditions relevant for the purposes of the first principle: Processing of sensitive personal data

1. The data subject has given his explicit consent to the processing of the personal data.
2. (1) 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.

(2) The Secretary of State may by order-
 - (a) exclude the application of sub-paragraph (1) in such cases as may be specified, or
 - (b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.
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
 - (c) 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

- (d) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.
7. (1) 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.
- (2) The Secretary of State may by order-
- (a) exclude the application of sub-paragraph (1) in such cases as may be specified, or
 - (b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.
8. (1) 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.
- (2) In this paragraph "medical purposes" includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.
9. The processing-
- (1) (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.
- (2) The Secretary of State may by order specify circumstances in which processing falling within sub-paragraph (1)(a) and (b) is, or is not, to be taken for the purposes of sub-paragraph (1)(c) to be 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