



HIGHLAND INFORMATION SHARING POLICY



October 2004

HIGHLAND POLICY FOR SHARING INFORMATION

INTRODUCTION

- 1.1 Background
- 1.2 Parties to the Policy
- 1.3 Scope

2 OBJECTIVES

3 GENERAL PRINCIPLES

- 3.2 Key Legislation and Guidance
- 3.2 Principals of information sharing

4 PURPOSES FOR WHICH INFORMATION WILL BE SHARED

5 DISCLOSURE OF PERSONAL INFORMATION

- 5.1 Obtaining consent
- 5.2 Recording consent
- 5.3 Checking for consent
- 5.4 Disclosing information without consent

6 ACCESS AND SECURITY PROCEDURES

- 6.1 Transfer of personal information
- 6.2 Use of personal information for purposes other than that agreed

7 MANAGEMENT OF PROCEDURES

- 7.1 Formal approval and adoption
- 7.2 Dissemination of Policy and Procedures
- 7.3 Monitoring and reviewing
- 7.4 Reporting breaches of protocols

CONTRACTUAL AGREEMENT

- 8.1 Undertaking
- 8.2 Signatures

APPENDIX A: Confidentiality Standard

HIGHLAND POLICY FOR SHARING INFORMATION

1. INTRODUCTION

1.1 Background

Sharing information about an individual between partner agencies is vital to the provision of co-ordinated and seamless services. Where information sharing has occurred, its value has often been reduced by such problems as misunderstandings in the use of language or inefficiencies in communication. These barriers have led to concerns and to uncertainties about the circumstances of information sharing.

3.3 Parties to the Policy

NHS Highland
The Highland Council
Northern Constabulary

It would be anticipated that other partners within the Wellbeing Alliance such as Communities Scotland, Scottish Natural Heritage and Highland and Islands Enterprise would also wish to adopt this policy.

3.4 Scope

3.4.1 The Highland partners' approach to Information Sharing consists of Individual Procedures supported by this Information Sharing Policy. Each Information Sharing context may require a specific set of procedures.

3.4.2 The need to share information between agencies has long been recognised within Highland. The Information Management and Technology (IM&T) strategies of the partner agencies recognise the need for shared information standards and robust information security to support the implementation of joint working arrangements. This policy has been developed by the Highland partner agencies, and adheres to the national model authorised by the Scottish Executive (SE).

4 OBJECTIVES

2.1 To provide a framework for the secure and confidential sharing of information between organisations to enable them to meet the needs of individuals for care, protection and support in accordance with government expectations and legislative requirements.

2.2 To inform service users of the organisations who are party to this policy, of the reasons why information about them may need to be shared and how this sharing will be managed.

3 GENERAL PRINCIPLES

3.1 Key Legislation and Guidance

3.1.1 Since 1 March 2000 the key legislation governing the protection and use of identifiable service user information (Personal Data) has been the Data Protection Act 1998 (www.dataprotection.gov.uk; www.hmsso.gov.uk/acts1998/19980029.htm). The DPA Act does not apply to information relating to the deceased.

- 3.1.2 The **Crime and Disorder Act 1998** (www.homeoffice.gov.uk/cdact/) introduces measures to reduce crime and disorder, including the introduction of local crime partnerships around local authority boundaries to formulate and implement strategies for reducing crime and disorder in the local area.
- 3.1.3 All staff working in both the statutory and independent sector are aware that they are subject to a **Common Law Duty of Confidentiality**, and must abide by this.
- 3.1.4 All partner agencies are subject to their own codes or standards relating to confidentiality (*see Appendix*).
- 3.1.5 **Freedom of Information (Scotland) Act 2002** (www.scotland.gov.uk/government/foi) legislation requires public authorities to put procedures in place to facilitate disclosure of information under the Act.
- 3.2 **Principles governing the sharing of information in Highland**
- 3.2.1 Initiatives requiring a multi-agency approach cannot be achieved without the exchange of information about individual service users, levels of activity, the level and nature of resources and how issues are addressed. Adoption of a multi-agency approach to address issues therefore, includes a commitment to enable such information to be shared, and in a manner compliant with statutory responsibilities.
- 3.2.2 Non-NHS organisations recognise the requirements that Caldicott imposes on NHS organisations and will ensure that requests for information from NHS organisations are dealt with in a manner compatible with these requirements.
- 3.2.3 All organisations accept this duty of confidentiality and will not disclose such information without the consent of the person concerned, unless there are statutory grounds and an overriding justification for so doing.
- 3.2.4 Organisations will use information only for the purpose established under the agreed procedures. Information shared with a member of another organisation for a specific purpose will not be regarded by that organisation as intelligence for the general use of the organisation.
- 3.2.5 Individuals in contact with organisations/agencies will be fully informed about information that is recorded about them. They will be given every opportunity to gain access to information held about them and to correct any factual errors that have been made.
- 3.2.6 Organisations are committed to putting in place efficient and effective procedures to address complaints relating to the disclosure of information, and service users will be provided with information about these procedures.
- 3.2.7 Organisations will ensure that all relevant staff are aware of, and comply with, their responsibilities in regard both to the confidentiality of information about people who are in contact with their organisation/agency and to the commitment of the organisations to share information.
- 3.2.8 Procedures will be put in place to ensure that decisions to disclose personal information without consent have been fully considered, and that these decisions can be audited and defended. All relevant staff will be provided with training in these procedures. Staff will be

made aware that disclosure of personal information, which cannot be justified, whether inadvertent or intentional, will be subject to disciplinary action.

- 3.2.9 Where it is agreed to be necessary for information to be shared, information will be shared on a need-to-know basis only.

4. PURPOSES FOR WHICH INFORMATION WILL BE SHARED

4.1 The purpose for information sharing is as follows:

- To improve the quality of services for people in Highland
- To produce consistent services and information
- To provide professionals with the information they need to deliver integrated services
- To support a single point of access and out of hours services for the community
- To support joint care planning and commissioning
- To support statutory reporting functions and effective use of resources
- To assist the management teams of Highland partner organisations with planning and management information
- To support national initiatives on multi-agency working and information exchange.

5. DISCLOSURE OF PERSONAL INFORMATION

5.1 Obtaining consent

5.2 Any member of staff who seeks consent to share personal information with other agencies will present and explain the issues, and will explain the consequences if consent is not given.

5.2 Consent will be sought at the earliest opportunity and given on an informed basis. This should be at the first contact with the person concerned unless the individual is unable, at that time, to fully comprehend the implications or make an informed judgement. Individual organisations' procedures will specify the circumstances under which the agency may exercise their right to disclose information without consent.

5.2 In order to ensure that consent to the sharing of personal information is informed, all agencies will have available material which explains:

- The rights of individuals under the Data Protection Act 1998.
- Details of the procedures in place to enable service users to access their records.
- Details of the specific procedures that may have to be initiated when a member of staff suspects that an individual has been or is at risk of abuse. These procedures must include details of whom information will be shared with at each stage, what information will be shared and how the information will be used.
- Details of the procedures that may have to be initiated must include details of whom information will be shared with at each stage, what information will be shared and how the information will be used.
- Details of the circumstances under which information may be shared without consent and the procedures which will be followed.
- Details of the complaints procedures to follow in the event that the individual concerned believes information about them has been inappropriately disclosed.
- Details of how the information they provide will be recorded, stored and the length of time it will be retained both by the point of contact agency and the agencies to which they may disclose that information.

- Details of the length of time for which consent to particular disclosures is valid.

5.2 **Recording consent**

- 5.2.1 Agencies must have a means by which an individual or their guardian can record whether they give consent to the disclosure of personal information and what limits, if any, they wish placed on that disclosure. This may be a consent form associated with the specific procedures. These limitations should be over-ridden only if there are statutory grounds for doing so.
- 5.2.2 Individuals should be able to prescribe, in respect of all information held by the contact organisation:
- Which organisations' information can and cannot be shared with
 - Whether the defined shared dataset can be shared or remain confidential.
- 5.2.3 In addition, in respect of sensitive information (as defined by the DP Act 1988) which is held by the contact organisation, individuals must be able to prescribe the explicit purposes for which they agree to this information being disclosed to another organisation.

5.3 **Checking for consent**

- 5.3.1 Before personal information is disclosed to another agency the person making that disclosure must check that consent has been given.
- 5.3.2 Organisations will be kept fully informed about the disclosure of information originating from their files, whether it is with or without the consent of the person to whom the information pertains. Accurate records must be kept of what information has been disclosed to whom, the source of the data disclosed, and the date on which it was disclosed, and procedures must specify who will be responsible for ensuring that this is done.

5.4 **Disclosing information without consent**

- 5.4.1 The disclosure of personal information without consent must be justifiable on statutory grounds.
- 5.4.2 Each agency will therefore appoint a person or persons who has the authority and knowledge to take responsibility for such a decision. This authority will be available at all times, to enable emergency situations to be dealt with.
- 5.4.3 If information is disclosed without consent, then full details will be recorded about the information disclosed, the reasons why the decision to disclose was taken, the person who authorised the disclosure and the person(s) to whom it was disclosed. Individual agency procedures will specify the person(s) responsible for ensuring this happens.
- 5.4.4 Recipients of the information will be made aware that it has been disclosed without consent and will put agreed security procedures in place.

7 **ACCESS AND SECURITY PROCEDURES**

6.1 **Transfer of personal information**

- 6.1.1 Organisations will nominate contacts for the receipt of personal and sensitive information. These contacts will be responsible for instigating the agreed security procedures to ensure that this information is restricted to those who need to know it for the purposes agreed. Individual procedures will detail the agreed contacts.
- 6.1.2 Fax transfer will be avoided wherever possible. Where it is necessary, then individual agency procedures for secure transfer by fax will be followed. It is recognised that in urgent cases, information about individual clients and/or patients may have to be requested or provided via the telephone.
- 6.1.3 Electronic transfer of personal information will only be permitted on a system to system basis across secure networks.
- 6.1.4 Written communications containing sensitive information should be transferred in a sealed envelope and addressed by name to the designated person within each organisation. They should be clearly and appropriately marked. The designated person should be alerted to the despatch of such information and should make arrangements with their own organisation to ensure both that the envelope is delivered to them unopened and that it is received within the expected timescale.

6.2 Use of personal information for purposes other than that agreed

- 6.6.1 Confidential information is disclosed only for the purpose specified at the time of disclosure and it is a condition of access that it should not be used for any other purpose without the consent of both the data owner and the data subject. The purpose is set out in the Individual Procedures and information should not be shared or used for any other purpose.
- 6.6.2 Partners wishing to use that information for any other purpose, or who wish to disclose that information to any person other than those authorised to receive the information, must submit a formal application to the data owner. It is the responsibility of the data owner to obtain the consent of the patient or client to the further use of that information or to decide whether the reason the information is required justifies disclosure without consent.

8 MANAGEMENT OF PROCEDURES

7.2 Formal approval and adoption

- 7.2.1 The Joint Committee for Action on Community Care will formally approve this policy. Individual Procedures will be signed off by the appropriate agencies. Formal adoption will follow the signing of the document by the head of each partner organisation. It is anticipated that the Wellbeing Alliance partners will also formally adopt the policy.

8.2 Dissemination of Policy and Procedures

- 7.2.1 The policy and Individual Procedures will be introduced to appropriate staff following internal agency training. Copies of the Policy and Individual Procedures will be circulated to all relevant staff, in line with each agency's internal arrangement for distribution of procedures and guidelines.

7.4 Monitoring and reviewing

- 7.4.1 All procedures will be subject to regular formal review, and legal advice will always be sought before any major changes are considered.
- 7.4.2 Each procedure will set out the particular arrangements for its review. These will include details of:
- The body responsible for reviewing and agreeing changes.
 - The date of the initial review and the review frequency.
- 7.4.3 Staff in all organisations will be required to log and report responses and behaviour which they believe are not in accordance with the procedures. All organisations will have a system by which complaints, regarding the inappropriate use or disclosure of information, are reported to the body responsible for the security of that information.

7.4 Reporting breaches of protocols

- 7.4.1 The following types of incidents will be logged:
- Refusal to disclose information.
 - Conditions being placed on disclosure.
 - Delays in responding to requests.
 - Disclosure of information to members of staff who do not have a legitimate reason for access.
 - Non-delivery of agreed reports.
 - Inappropriate or inadequate use of procedures e.g. insufficient information provided.
 - Disregard for procedures.
 - The use of data/information for purposes other than those agreed.
 - Inadequate security arrangements.
- 7.4.2 A member of staff, in any of the organisations party to this policy, who becomes aware that the procedures and agreements set out are not being adhered to, whether within their own or a partner organisation, should first raise the issue with the line manager responsible for the day-to-day management of the procedures.
- 7.4.3 Individual Procedures should detail the mechanism by which breaches will be reviewed, addressed and resolved. A log should be maintained of breaches to enable review of the procedures.
- 7.4.4 Breaches alleged by a member of the public:
- 7.4.4.1 Any complaint received by, or on behalf of, a member of the public containing allegations of inappropriate disclosure of information will be dealt with, in the normal way, by the internal complaints procedures of the organisation that received the complaint. Any disciplinary action will be an internal matter for the organisation concerned.

8 CONTRACTUAL AGREEMENT

8.2 Undertaking

- 8.2.1 The parties to the policy accept that the standards laid down in this document will provide a secure framework for the sharing of information between their agencies in a manner compliant with their statutory and professional responsibilities.

8.1.2 As such, they undertake to:

8.1.2.1 Implement and adhere to the procedures and structures set out in this policy.

8.1.2.2 Ensure that all INDIVIDUALPROCEDURES established between their agencies for the sharing of information relating to the population of the Highlands are consistent with this POLICY.

8.1.2.3 Ensure that where these procedures are adopted then no restriction will be placed on the sharing of information other than those specified within INDIVIDUAL PROCEDURES.

8.2 Signatures

8.2.1 We, the undersigned, agree to adopt and adhere to this information sharing policy:

Organisation:	Designation:	Name:	Date:
The Highland Council	Head of E Government	John Tyreman	
Highland Primary Care Trust	Head of Information Services	William T Reid	
Northern Constabulary	Information Security Officer	I A Williams	
NHS Highland	Head of Statistical Services	P C Hopkins	
Highland Acute NHS Trust	Medical Director	Alison Graham	

APPENDIX A: Confidentiality Standards

This section contains each organisation's codes or standards relating to confidentiality:

Highland Council

e.g. Corporate Information Strategy; Information Security Policy Statement; Communications Policy; General Computer Security Policy; Data Protection Policy; Data Protection Subject Access Guide; Access to your Information leaflet; Email Security Policy; Internet Security Policy.

Highland NHS Bodies

e.g. Information, Management and Technology Strategy; Information Security – Information Technology Security Policy; Intranet, E-mail and Internet Services – Access Terms and Conditions; E-Mail Services – Policy.

Northern Constabulary

Force Reference Documents: Information Security; Data Protection; Information Technology; Protective Marking.

HIGHLAND POLICY FOR SHARING INFORMATION

Sign-off Circulation Record

Name – Data Protection Officer	Organisation	Date Received	Date Sent On	Sign