Scottish Accord on the Sharing of Personal Information

Information Sharing Protocol

Between

The Scottish Ministers, Acting through the Scottish Prison Service and

NHS Ayrshire & Arran,
NHS Dumfries and Galloway
NHS Forth Valley
NHS Grampian
NHS Greater Glasgow and Clyde
NHS Highland
NHS Lanarkshire
NHS Lothian and
NHS Tayside

Collectively known as 'NHS Scotland' for the purposes of this information sharing protocol

Version: 0.8 (final version)

INFORMATION SHARING PROTOCOL

INTRODUCTION

This document is a binding agreement for data sharing between the Scottish Prison Service (SPS) and NHS Boards, hereafter referred to as 'partners'.

Effective data sharing is the key to multi-agency working in any sphere and the Partners positively encourage their staff to share information appropriately about their service users when it benefits their care and when it is necessary to protect vulnerable adults.

This agreement outlines the terms and conditions agreed between the partners under which identifiable information needs to be shared and the safeguards that must be implemented. The agreement exists to ensure that data can be shared in a way which satisfies both the legal and professional obligations of the partners, their respective staff and the legitimate expectations of the data subjects.

This agreement includes the transfer of information for prisoners by 3rd party contractors.

This document adheres to the Data Sharing Code of Practice issued by the Information Commissioner (Regulator for the Data Protection Act 1998) in May 2011.

On behalf of our respective organisations, we accept and endorse this agreement.

Signed by Chief Executive on behalf of:

NHS Ayrshire & Arran **DATE**

NHS Dumfries and Galloway **DATE**

NHS Forth Valley **DATE**

NHS Grampian **DATE**

NHS Greater Glasgow and Clyde **DATE**

NHS Highland **DATE**

NHS Lanarkshire **DATE**

NHS Lothian **DATE**

NHS Tayside **DATE**

Signed on behalf of Scottish Ministers/SPS

(Chief Executive)

Content

ANNEX List

Part A – Introduction to this ISP

1 Scope and purpose of this ISP

1.1 This Information Sharing Protocol (ISP) is supplementary to the Memorandum of Understanding (MOU), and has been agreed between the participating partner organisations. Partners have given consideration to its contents when drawing up this document. SPS Memorandum of Understanding

1.2 This ISP has been prepared to support the regular sharing of personal information for prisoner-patients including those in courts, with a view to supporting their care and case management in prisons and their transition in and out of prison.

1.3 It supports the information sharing partner organisations involved and the groups of Service Users it impacts upon. It details the specific purposes for sharing and the personal information being shared, the required operational procedures, and legal justification.

1.4 The aims of the agreement are as follows:

- To support healthcare for prisoner patients.
- To support integrated care and case management.
- To support community reintegration.
- To support transition from the community, through police and courts, into prison and their release back out into the community.
- Continuous improvement of services.
- To protect confidentiality.
- To comply with the law and good practice on information sharing.

1.5 Information may also be shared to support the effective administration, audit, monitoring, inspection of services and reporting requirements. This information will be anonymised wherever possible. Partners may only use the information disclosed to them under this ISP for the specific purpose(s) set out in this document. Partners agree only to use the information disclosed to them under this agreement and will not further use the data unless in compliance with Data Protection legislation.

1.6 This agreement includes the transfer of information for prisoners by 3rd party contractors.

2 High level functions of this ISP

2.1 The functions which this information sharing protocol community are seeking to support, include but are not limited to:

- Healthcare in prisons.
- Integration of care in and out of prisons.
- Government ambitions on ‘Safer’ and ‘Healthier’.
- Performance monitoring and Government-based target setting.
- Prisons’ mission of care and opportunity, integration, safe custody and good order.
- Health Improvement.
- National reporting.

3 Service Users included in this ISP

3.1 The Service Users which this ISP relates to include:

- The agreement relates to prisoners in custody in Scottish prisons.

4 Benefits to Service Users

4.1 The health needs of current and future prisoners should be addressed safely, effectively, equitably and, as far as is appropriate, in partnership with patients who are prisoners. The Information Sharing Protocol enables the quality of care to be assessed and assured across and between agencies and that the information held about individuals is accurate.

4.2 Benefits to the Service Users include:

- Supports direct patient care;
- Supports integrated and critical areas of care and case management;
- Supports governance and assure quality of prison-based health services and their integration with community-based health services and prison-based non-health services;
- Involves prisoners in decisions about their health and care;
- Ensures information held about them is accurate.

5 Details of personal information being shared

5.1 Personal information shared for the purpose of this ISP includes a range of information regarding the Service Users needs.

5.2 The information is used to facilitate operational prison management and the ongoing management and review of a prisoner's health and social care. The information shared may therefore include:

- Clinical Information
- Health risks e.g. notifiable or communicable diseases
- Suicide risk management
- SPS Integrated case management (ICM)
- Social and safety risks, to other prisoners and the public, e.g. parole dossier
- Risks to staff
- Demographic details including ethnicity and belief
- Location information
- Relevant legislation e.g., adult support and protection, child protection
- Critical incident review

Only the **minimum necessary** personal information consistent with the purposes set out in this document will be shared. Sensitive information shared will be the minimum required for the intended purpose (as per section 1.5).

6 Key identifying information

6.1 When sharing information, the following identifiers will be used where available, to ensure that all partner organisations are referring to the same prisoner:

The key identifying information is:

1. Prisoner number (SPIN)
2. Community Health Index (CHI)
3. Name
4. Address
5. Date of Birth
6. Gender

7 The information sharing partner organisations

Annex A lists the organisations covered by this ISP.

7.1 This ISP covers the exchange of information between the organisations detailed in Annex A that are engaged in delivering the service outlined in this document:

7.2 As well as those organisations identified in Annex A it is acknowledged that each of the Data Controllers have existing arrangements with other external organisations in terms of service provision where the processing of health information is being carried out under Data Controller/Data Processor contracts.

7.3 The responsible managers have overall responsibility for this ISP within their own organisations, and must therefore ensure the ISP is disseminated, understood and acted upon by relevant staff.

7.4 Staff of these partner organisations who work directly with prisoners in order to carry out the functions described in this ISP, are bound by this document.

7.5 The term ‘staff’ encompasses paid workers, volunteers, students and other temporary workers approved by the employing / hosting organisation, whose duties include those relating to the functions outlined in this ISP.

7.6 Partner organisations will ensure that all current and newly-appointed staff receives appropriate training in Information Governance requirements.

Part B – Justification for sharing personal information

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.

8 Legislative / statutory powers

8.1 Disclosure of information will be conducted within the legal framework of the Data Protection Act 1998 (DPA), the Human Rights Act 1998 and in compliance with the common law duty of confidence.

8.2 Both SPS and NHS Boards are under a Duty of Care to look after prisoners under their care. This Duty of Care provides the legal basis for the partners to share prisoners' personal information **without** obtaining their consent where relevant and appropriate. Only the **minimum necessary** personal information consistent with the purposes set out in this document will be shared. Sensitive information shared will be the minimum required for the intended purpose.

8.3 Relevant legislation includes but is not restricted to:

- Access to Health Records Act 1990
- Adults with Incapacity (Scotland) Act 2000
- Adult Support and Protection (Scotland) Act 2007
- Child Protection (Scotland) Act 1995
- Criminal Justice (Scotland) Act 2003
- Criminal Procedures (Scotland) Act 1995
- Freedom of Information (Scotland) Act 2002
- Health Board Guidance on Provision of Healthcare to Prisoners in Prison (known as Prison Healthcare Guidance)
- Health Board Provision of Healthcare in Prisons (Scotland) Directions 2011 (known as The Prisons Directions)
- Management of Offenders (Scotland) Act 2005
- Mental Health Care and Treatment (Scotland) Act 2003
- Multi-agency Public Protection Arrangements (MAPPA) 2007
- National Health Service Reform (Scotland) Act 2004
- NHS Circular PCA(M)(2011) 15
- The Prisons and Young Offenders Institutions (Scotland) Rules 2011
- Social Work (Scotland) Act 1968

8.4 **Data Protection Act 1998 and the Human Rights Act 1998**

Disclosure of data will be conducted within the legal framework of the Data Protection Act 1998, the Human Rights Act 1998 and in compliance with the common law duty of confidence, underpinning how the sharing of information is controlled, where consent is not required.

The Data Protection Act 1998 requires that data controllers meet certain obligations, which include compliance with the eight data protection principles. The first data protection principle states that personal data shall be processed fairly and lawfully and shall not be processed unless at least one Schedule 2 condition and, in the case of 'sensitive personal data', at least one Schedule 3 condition is also met.

The partners to this agreement confirm that their processing of personal data complies with the requirements of Schedules 2 and 3 of the Data Protection Act 1998 as follows:

- Schedule 2, Para 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. Schedule 2 paras 3, 4 and 5 (a), (b) and (d) may also be relevant in restricted circumstances.
- Schedule 3, Para 8: The processing is necessary for medical purposes and is undertaken by a health professional or others owing an obligation of confidence to the data subject. Schedule 3 paras 7 (a) and (b) are also relevant.

In terms of the Data Protection Act 1998, the role of data controller between the partners will vary depending on which information sharing is taking place. For examples see Annex B.

8.5 **Caldicott Principles**

Caldicott Guardians are appointed to oversee the arrangements for the use and sharing of patient identifiable information across all NHSScotland organisations.

Whilst the legal provision for the work of the Caldicott Guardians is primarily the Data Protection Act 1998, NHS staff should ensure compliance with the Caldicott principles when sharing information. These are:

- Principle 1 - Justify the purpose(s) for using confidential information
- Principle 2 - Only use it when absolutely necessary
- Principle 3 - Use the minimum that is required
- Principle 4 - Access should be on a strict need-to-know basis
- Principle 5 - Everyone must understand his or her responsibilities
- Principle 6 - Understand and comply with the law

9 Consent

9.1 For the purposes of this protocol and the processes described in it no consent will be required from Service Users.

9.2 For the purpose of this protocol and the processes described in it

- the Duty of Care provides the legal basis for the partners to share prisoners' personal information
- the Data Protection First Principles requirements are met in as much as
    - fair processing information is being provided
    - Schedule 2, Conditions paragraphs 3, 4 and 5 (a,b,d) and (d) 6(1) apply
    - Schedule 3, Condition 7 (a,b) and 8 apply in relation to processing personal information **without** obtaining the individual's consent

9.3 Compliance with the Data Protection Act 1998 is addressed at section 8.3 above.

9.4 Partner organisations should be prepared to be open with their prisoners about the reasons and justifications that are relied on to process their information.

9.5 If there is a significant change in the use to which the information will be used compared to that which had previously been explained, or a change in the relationship between a partner organisation and the prisoner, then these conditions and their relevance to consent will be re-assessed.

Part C – Operational procedures and guidance for this ISP

This protocol will assist in identifying the key procedures and safeguards that will be used to allow the legal and secure sharing of information between the partner agencies in providing joint services to their users.

Secure sharing is facilitated by point to point transfer e.g. encryption, use of lockable, traceable tamper proof bags and locked briefcases. Where fax is used (which should not be common practice) it should be an approved secure fax (SAFE HAVEN).

10 Summary

10.1 Only the minimum necessary personal information will be shared on a **need-to-know** basis and only when it supports the delivery of the purposes and functions set out in this ISP.

10.2 Personal information will only be collected using the approved collection methods, ensuring the required information is complete and up-to-date.

10.3 All reasonable steps must be taken to ensure that anyone who has received information is notified of any relevant changes and if any inaccuracies are found the necessary amendments will be made.

10.4 Decisions about prisoners should never be made by referring to inaccurate, incomplete or out-of-date information.

10.5 Staff must also follow their own organisation's procedures relating to the handling of personal information.

10.6 **Staff and Others with Access to Information** - 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 partners, its managers and practitioners, and compliance with Caldicott Principles.

10.7 Staff contracts must contain appropriate confidentiality clauses that detail possible consequences of unauthorised or inappropriate disclosure of personal identifiable information.

10.8 Each organisation must ensure that all relevant staff receive regular Information Governance training, advice and ongoing support in order to be made aware, and understand the implications, of:

- This ISP and the operational protocol. This should include any associated operational requirements arising from their implementation;
- The Data Protection Act, the Human Rights Act, the Common Law Duty of Confidentiality and Caldicott Principles;
- Codes of Practice and any other associated regulations and guidance including advice on safe, secure, accurate and appropriate data collection, storage, transfer, analysis, archiving and destruction of data.

10.9 Each organisation must have in place equitable disciplinary, audit and investigative procedures which may be invoked if a member of staff is found to have breached the confidentiality of a prisoner or to have shared information in a manner in contravention of this ISP.

10.10 Where a partner relies on a third party to process personal information the organisation must have in place appropriate contractual data processing and confidentiality agreements in line with CEL 25 (2011) Safeguarding the Confidentiality of Personal Data Processed by Third Party Contractors which applies within the NHS.

10.11 Each organisation must consider and document the impact on individuals' privacy before developing any new IT system or changing the way they handle personal information.

10.12 There should be an audit system in place that allows inappropriate access to be detected and investigated in a systematic and non-discriminatory way.

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.

11 Fair processing information

11.1 Each organisation must inform prisoners 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, at the earliest appropriate opportunity preferably at first contact. This is known as a 'Fair Processing or Privacy Notice'.

11.2 The following information, as a minimum will be provided to the prisoner:

- The identity of the party whose notice it is
- The fact that the parties work jointly to provide improved services

11.3 Each organisation must ensure that they have 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 prisoners in a fair and consistent manner and in accordance with any specific legislative requirements, regulations or guidance.

11.4 Each organisation must also inform prisoners about their rights, in respect of legislation and how these may be exercised. This will include the provision of appropriate support in order that prisoners 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.

11.5 Agreed methods of providing this information are:

- Patient registration form
- Verbally
- Information sharing leaflet e.g. the Health Rights Information Scotland (HRIS) Leaflets
- Posters and forms

12 Obtaining consent

12.1 For the purposes of this ISP no consent will be required from Service Users.

12.2 This Duty of Care provides the legal basis for the partners to share prisoners' personal information **without** obtaining their consent where relevant and appropriate.

12.3 Partner organisations should be prepared to be open with their prisoners about the role that their consent plays in the information sharing process and indeed be clear about the type of circumstances in which they may share personal information without their knowledge or consent.

12.4 If there is a significant change in the use of information compared to that which had previously been explained, or a change in the relationship between a partner organisation and the prisoner, then consent will be sought.

13 Actions to be taken where a Service User lacks mental capacity

Also, refer to section 12.4.

13.1 The Adults with Incapacity (Scotland) 2000 Act and codes of practice defines the term 'a person who lacks capacity' as a person who lacks the capacity to take some or all decisions for themselves because of mental disorder or inability to communicate by any means.

13.2 Whenever dealing with issues of capacity to understand the nature of this personal information processing, local rules and procedures should be followed and these must be compatible with the Adults with Incapacity (Scotland) 2000 Act and codes of practice.

14 Temporary impairment of capacity

Also, refer to section 12.4.

14.1 Where a person has a temporary loss of capacity the processing of their personal information will continue where it is consistent with Section 9. Relevant information about the nature of this personal information processing will be provided when capacity is regained.

15 Information collection

15.1 The approved collection tools for partner organisations to gather the personal information detailed in this ISP may include but not be limited to:

- INPS Vision (NHS)
- PR2 (SPS)
- Associated NHS electronic applications (NHS)
- Manual records (SPS and NHS)
- Share Point (SPS)
- GP records (NHS)
- Parole Dossier (SPS)

Information will be shared between SPS and NHS through a number of different processes:

- **Data transferred electronically from PR2 to NHS eLinks Ensemble**

  will consist of prisoners' personal demographic data to populate INPS Vision as agreed by both parties.

- **NHS health professionals accessing PR2 to read fields** – NHS staff with appropriate permissions based on User Roles will be able to access the SPS PR2 prisoner database to read certain fields.

- **SPS staff accessing ACT2Care records** – SPS staff will be able to access ACT2Care documentation contained in the health record, in the presence of a healthcare professional.

- **Sentence Management, Warrant information, ACT history** – The Criminal Desk in each prison will provide paper documents to the local NHS health centre staff.

- **Transfer of Health Care Records and ACT Documentation accompanying prisoner on transfer to another prison** – The Prison Escort contractor (acting on behalf of SPS) will transport the prisoner's health records along with the prisoner when the prisoner is transferred from one prison to another prison.

- **Prisoners under escort from a prison (health information)** - The Prison Escort contractor (acting on behalf of SPS) will transport the prisoner's health information along with the prisoner when the prisoner is under escort e.g. for a hospital appointment.

  The safety of the public, staff and prisoners should be managed as part of this process. Where available, appropriate information should be shared to ensure their safety.

- **Parole Board Reports**

  NHS staff providing or completing the healthcare report as a contribution to the prisoner parole dossier.

- **Assaults KPI**

  Relevant data to inform SPS management to measure corporate KPI.

15.2 **Protective Marking**

Sensitive personal data as defined in the Data Protection Act 1998 is personal data consisting of information as to:

a) racial or ethnic origin of the data subject,
b) political opinions,
c) religious beliefs or other beliefs of a similar nature,
d) trade union membership,
e) physical or mental health or condition,
f) sexual life,
g) the commission or alleged commission of any offence, or
h) any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

In particular, any information shared between SPS and NHS which includes data on the prisoner's ***physical health, mental health or condition*** must be treated as sensitive personal data.

Sensitive personal data must be protectively marked as follows:

- SPS will use the Government Protective Marking Scheme (GPMS) and will mark sensitive personal data as **RESTRICTED**;
- NHS will use the NHS Protective Marking Scheme and will mark sensitive personal data as **NHS CONFIDENTIAL**.

Protectively marked information will be provided on the understanding that it will be stored, transferred and destroyed in accordance with the information security requirements described below.

15.3 **Document Marking**

Where possible, documents should be clearly marked with the protective marking. Each page should be marked at both the header and the footer using embolden capital letters – for example **RESTRICTED** or **NHS CONFIDENTIAL**. File covers should be similarly marked.

15.4 **Storage**

Protectively marked documents must be stored in a locked cabinet in a secure building.

15.5 **Mail**

Protectively marked documents that are being mailed internally or externally should be double enveloped. The inside envelope should have the name and address of the intended recipient and the protective marking. The outside envelope should have the name and address of the intended recipient and a return address in the event that the delivery cannot be made. The outer cover should not show the protective marking.

Sensitive personal data sent externally should be carried by trusted hand or sent using a courier or via the accepted Health Board procedures.

15.6 **Email**

Emails between NHS and SPS containing sensitive personal information should be appropriately marked:

- in the subject box at the beginning or end of the title using capital letters; and
- in the message text at the start or top of the e-mail using embolden capital letters.

Personal or sensitive data may only be exchanged by e-mail if both the sender and the recipient's e-mail addresses indicate that they are on email networks that are accredited to carry emails at that level of sensitivity. Data marked RESTRICTED, PROTECT or NHS CONFIDENTIAL may only be sent from and to email addresses containing:

- *.pnn.gov.uk; or

- *.nhs.net

Once received in organisation, safe email transfer procedure should be followed in line with local policy. The sender should ensure that recipients are aware of how protectively marked information should be handled and, ideally, obtain confirmation that the intended recipient agrees to the handling conditions prior to sending.

15.7 **Fax**

In general fax machines should not be used for sending protectively marked information and should only be used if absolutely necessary.

If it is considered essential to send protectively marked information by fax then the following procedures should be followed:

- Fax machines should be located in a secure area and operated by users who fully understand their responsibilities for maintaining confidentiality;
- Wherever possible, the room housing the fax machine should be locked when unattended or not in use;
- Clinical information should not be faxed. However if this is unavoidable, a unique person identifier such as the CHI number or hospital case record number should be used and all other personal identifiers removed;
- To minimise the risk of mis-dialling store the fax number of the recipient in the fax machine and then only use the number stored in the machine to send the fax;
- Ensure a trusted recipient is present at the receiving fax machine to accept the fax;
- Send the cover sheet first and wait for confirmation that it has arrived;
- Send the remainder of the fax and wait for confirmation that it has been received;
- All faxes should be pre-fixed with a standard front cover sheet detailing a confidentiality warning, number of pages and disclaimer notice;
- Approved secure fax or NHS Safe Havens should be used as available.

15.8 **Telephone**

Before providing confidential patient information over the telephone staff should:

- Confirm the name, job title, department, organisation and switchboard number of the person requesting the information and also the reason for the information request, if appropriate.
- Information should not be given out by telephone unless completely satisfied of the identity of the caller and their entitlement to the information.
- Unless the caller is well known to you, his/her identity should always be established by ringing the person back (via a manned switchboard – not dialling the number they have provided and never to a mobile)

- Check whether the information can be provided and if in doubt, tell the enquirer you will call them back.
- Ensure you record your name, date and time of disclosure, the reason for it and who authorised it. Also record the recipient's name, job title, organisation and telephone number and determine:
  - who is making the enquiry?
  - whether they are authorised to have such information?
  - why they need such information?

In order to confirm the identity of a telephone caller, it may be necessary to ask for their contact details and to call them back via the central switchboard.

15.9 **Outside of the Office**

Sensitive personal information removed from the office for meetings or approved home working should be carried in accordance with local organisational information security procedures and should be the restricted minimum required.

15.10 **Retention and Secure Disposal**

All participating organisations will have a policy document which will make clear their approach to retention, storage and disposal of records, in line with the Public Records (Scotland) Act 2011 and the NHS Scotland Records Management Code of Practice, including the minimum retention schedules.

The organisations will ensure that their retention schedules (particularly relating to the shared information) will be subject to periodic review to ensure that the information is kept no longer than is legitimately required.

The organisations will have established mechanisms for archiving information which they require to retain for a period but which is not required for normal operational use. Such archiving helps comply with respect for the privacy of prisoners by significantly reducing the number of individuals with potential or actual access to the information.

Once documents containing sensitive or personal data are no longer required they must be shredded. Electronic data that is no longer required must be deleted or archived as appropriate, and electronic media (e.g. CDs or memory sticks) must be securely disposed of in line with local policy.

Archiving should be implemented in line with Scottish Government guidelines.

16 Frequency of information sharing

16.1 The personal information outlined within section 5, will be only be shared on a need-to-know basis to support the functions of this ISP.

16.2 Partner organisations will share relevant personal information as detailed in the Annex C to the Information Sharing Protocol which sets out a detailed description of the personal information to be shared between the partner organisations and includes:

- with whom in each partner organisation it will be shared;
- when it will be shared;
- why it will be shared; and
- the methods by which it will be shared.

The table will be reviewed one year after implementation and within three years thereafter or sooner if appropriate.

17 Information security

17.1 Breaches of security, confidentiality and other violations of this ISP must be reported in line with each partner organisations' incident reporting procedures, and to partners as appropriate.

17.2 The minimum information security requirements are as follows:

- Access to personally identifiable data (PID) is restricted to users who have the authority to see PID. This can include video or photography.
- Sensitive PID on computer screens or in hard-copy format must not be accessible by non-authorised individuals.
- Documents or electronic media (e.g. CDs or memory sticks) containing PID must be encrypted and stored in lockable, secure containers when not in use.
- Mobile devices must meet NHS (NHSScotland Mobile Data Protection Standard) or SPS information security policies for handling and encryption.
- Emails containing sensitive personal information must only be sent to and from email addresses containing *.pnn.gov.uk; or *.nhs.net. or in line with local organisational safe email policy.
- Data taken from premises must be kept secure at all times, must not be made available to individuals who are not authorised to see it, and must only be used for the purposes specified within the agreement. Secure file transfer should be used as appropriate.
- Once a paper document is no longer required, it must be destroyed as confidential waste. Electronic media must be securely disposed of when no longer required in line with local IT procedures.

18 PUBLIC INFORMATION REQUESTS

18.1 Data Protection Act – Subject Access Requests

Under the Data Protection Act 1998 a data subject (or authorised individuals acting on their behalf) has the right to make a Subject Access Request and to receive a copy of the personal data relating to them which is processed by an organisation. Dealing with such requests is the responsibility of each individual data controller. Communication must take place speedily to ensure the request is processed within the statutory 40 calendar day time period.

18.2 Freedom of Information (Scotland) Act – Information Requests

The Health Boards and the Scottish Prison Service are Scottish Public Authorities for the purposes of the Freedom of Information (Scotland) Act 2002 (FOISA) and are therefore obliged to respond within twenty working days to any request for information submitted to them in a permanent form e.g. a letter or email. All organisations are required to produce and maintain a Publication Scheme that is proactively published in accordance with the terms of FOISA. This will include publication of this agreement on their websites.

Any request for information submitted to either organisation will be processed under the organisations existing FOISA handling procedures, passing up through the organisations internal review process where appropriate.

Where any freedom of information requests are received which affect more than one partner or which are potential mixed Data Protection and Freedom of Information Act requests, the partners will liaise to ensure a consistent approach, particularly regarding any exemptions which may need to be applied and the justifications for them (e.g. concerning data which might have commercial implications or which may have been provided in confidence). The partners will ensure that any personal data exchanged between them in such situations continues to be on a strict 'need to know' basis.

18.3 Public Records (Scotland) Act 2011

The Health Boards and Scottish Prison Service are Scottish Public Authorities and therefore must have a records management plan setting out the proper arrangements for the management of the authority's public records. This plan must be submitted to the Keeper for agreement.

19 Complaints

19.1 Each partner organisation has a formal procedure by which prisoners can direct their complaints regarding the application of this ISP.

19.2 Any concerns or complaints received from prisoners relating to the processing or sharing of their personal information will be dealt with promptly and in accordance with the internal complaints procedures of organisations.

20 MANAGING THE AGREEMENT

20.1 Structure of the Agreement

The information sharing agreement is in four parts

- **Part A: Introduction to this Information Sharing Protocol (ISP**
- **Part B: Justification for Sharing Personal Information**
- **Part C**: **Operational Procedures and Guidance for this ISP**
- **Part D**: **Methods and controls for the sharing of personal information to support this ISP**

20.2 Management Structure

The Information Sharing Protocol will be signed by Chief Executives of the partners. This agreement will be managed by the local recognised SPS/NHS Prison Healthcare Liaison Groups within each NHS Board.

Urgent local matters should be addressed by the NHS Board Information Governance Manager and the appropriate contact at Scottish Prison Service HQ in the usual way. Any other material that has a potential national implication should be referred to the NPHN.

20.3 **Dispute Resolution**

If circumstances arise in which one partner has concerns in relation to the operation of this agreement every effort should be made to resolve this so that data exchange is not disrupted.

Serious operational concerns should be escalated to the nominated contacts and onward to the Chief Executive.

21 Breaches

21.1 The organisations will each ensure that the other party is promptly notified of any security breaches or significant security risks, affecting shared information. Where the breach is considered significant the Information Commissioner's Office will also be notified by the Data Controller(s). For a data breach, the Data Controller(s) involved will consider on a case by case basis whether to notify the affected individuals of that breach. This will include seeking clinical and security advice where appropriate.

21.2 Disclosure of data to persons/ agencies outside the terms of this agreement (for instance, the forwarding of e-mails containing data marked RESTRICTED or NHS CONFIDENTIAL to any individual or organisation which is not a signatory to this agreement) will be deemed to constitute a breach of the agreement, unless a clear, legal justification and evidence can be provided to support the disclosure.

22 Review of this ISP

22.1 This ISP and the OP will be version controlled and reviewed by NPHN or as legislation dictates.

Part D – Methods and controls for the sharing of personal information to support this ISP

23 Information flow reference table

23.1 Annex C provides a list of the personal information to be shared between the partner organisations, with whom in each partner organisation it will be shared with, when it will be shared, why it will be shared and the methods of how it will be shared.

23.2 The information flow reference table will be reviewed and updated as necessary, to reflect any changes in the processing of personal information detailed in this ISP.

Annex A

Information Sharing Partner Organisations	Responsible Manager
Scottish Prison Service (SPS)	Head Office, Health Strategy Manager
Scottish Prison Service (SPS) Prisons	
Aberdeen	The Governor
Addiewell	The Governor
Barlinnie	The Governor
Castle Huntly	The Governor
Cornton Vale	The Governor
Dumfries	The Governor
Edinburgh	The Governor
Glenochil	The Governor
Greenock	The Governor
Inverness	The Governor
Kilmarnock	The Governor
Low Moss	The Governor
Perth	The Governor
Peterhead	The Governor
Polmont	The Governor
Shotts	The Governor
NHS Boards	
NHS Ayrshire & Arran	Information Governance Lead
NHS Dumfries and Galloway	Information Governance Lead
NHS Forth Valley	Information Governance Lead
NHS Grampian	Information Governance Lead
NHS Greater Glasgow and Clyde	Information Governance Lead
NHS Highland	Information Governance Lead
NHS Lanarkshire	Information Governance Lead
NHS Lothian	Information Governance Lead
NHS Tayside	Information Governance Lead

Annex B

In terms of the Data Protection Act 1998, the role of data controller between the partners will vary depending on which information sharing is taking place. For example:

- **Transfer of information from SPS to NHS Scotland** (i.e. from PR2 to VISION) – In this case SPS and NHS each act as Data Controllers. Once data has been transferred from SPS to NHS, then NHS becomes entirely responsible for keeping the information secure and SPS is not responsible for any loss or damages arising from the use of the data by NHS.
- **NHS Scotland staff accessing the SPS PR2 database** - In this case SPS and NHS act as Data Controllers in Common because they share a pool of personal data that they process independently of each other. SPS will be responsible for keeping the information secure.
- **SPS staff accessing ACT2Care records** - In this case SPS and NHS each act as Data Controllers in common. ACT documentation is contained within the health record. NHS is responsible for the record management of the health record, incorporating ACT documentation.
- **SPS storing manual prisoner health records** - In this case NHS is the Data Controller and SPS is responsible for provision of the storage area. NHS is responsible for ensuring that the records are held securely.

ANNEX C – DETAILS OF DATASETS AND DATA FLOWS

	Description	Data Exchange 1			
1 a	**High Level Function(s)** General description of the function(s) or service(s) to which the data relates.	NHS prison health centre medical staff accessing PR2 to view fields (read access).			
2 a	**What data will be shared** Description of the data to be provided.	Case Management, identification, location, appointments, medical, security and other information.			
3	**Personal Identifiers included in the above** Main identifiers being used to identify the individual.	Surname	X	First Name	X
		Date of Birth	X	Address	X
		Prisoner No	X	Post code	X
		CHI		NHS No.	
		GP Code		Gender	
4 a	**Provider organisation(s) - (Who from)** Provider organisation(s).	SPS			
b	Directorate(s) or department(s) responsible for providing the data.	Local prison authorises access			
c	Roles of staff responsible for providing the data.	varied, accountable to the Governor in charge			
5 a	**Destination organisation(s) - (Who to)** Recipient organisation(s) with whom this data will be shared.	Health Board			
b	Directorate(s) or Department(s) responsible for receiving the data.	Health Board			
c	Roles of staff receiving the data.	Prison Health Centre staff			
6 a	**Reason(s) for use of the data - (Why)** Description of why the data is required e.g. law, care of individual.	Duty of Care to provide medical support to each prisoner			
7 a	**Source of data (What system)** Description of the data system(s), from which the data to be exchanged, is obtained.	PR2 (SPS Prisoner Records Database)			
b	Description of the module or fields accessed when using another organisation's IT system to share data.	Case Management, identification, location, appointments, medical, security and other information modules within PR2.			
8 a	**Form title and reference number - (What form)** The title and reference number of any form or letter used to convey and / or collect the data.	N/A			
9 a	**Destination record(s) / system(s) - (Where to)** The data system(s), record(s) or other destination of the data shared.	N/A			
10 a	**When exchanged / shared (When)** Details of when the data needs to be exchanged / shared e.g. daily, weekly, monthly, yearly, as and when.	Daily		Weekly	
		Monthly		Weekly	
		When required	X	Other	
11 a	**Communication media (How)** Details of all formats in which the data is to be transferred to the recipient e.g. direct feed from system, verbal transfer at team meeting, telephone call, e-mail.	Telephone		Fax	
		Face to face		Email	
		Direct feed from IT system		Access to paper record	X
		Access to IT system	X	Copy of paper record	X
		Letter or		Other	

		similar			
12 a	**Communication media controls (How)** Details of how all security controls are applied, e.g. password protected files, encryption of files, including any risks assessments undertaken.	Password protected access. Access based on User Roles.			
13	**Issues or comments not included in the above**				

ANNEX C – DETAILS OF DATASETS AND DATA FLOWS (contd.)

	Description	Data Exchange 2				Data Exchange 3			
1 a	**High Level Function(s)** General description of the function(s) or service(s) to which the data relates.	NHS medical staff accessing PR2 to update fields (write access).				SPS staff accessing ACT2Care records			
2 a	**What data will be shared** Description of the data to be provided.	Integrated Case Management, Sentence Management, Community Integration Plan, Liberation Scroll, prisoner appointments, activities, tribunals, HDC, service provider referrals, prisoner referrals, BCPs, ACT, risk and conditions, complaint history, generic searches, Operations, height and weight				Health Care Record, Warrant information, ACT Record			
3	**Personal Identifiers included in the above** Main identifiers being used to identify the individual.	Surname	X	First Name	X	Surname		First Name	
		Date of Birth	X	Address	X	Date of Birth		Address	
		Prisoner No	X	Post code	X	Prisoner No		Post code	
		CHI	X	Other SPS	X	CHI		Other SPS	
4 a	**Provider organisation(s) - (Who from)** Provider organisation(s).	Health Board							
b	Directorate(s) or department(s) responsible for providing the data.	Health Board							
c	Roles of staff responsible for providing the data.	Prison Health Centre staff.							
5 a	**Destination organisation(s) - (Who to)** Recipient organisation(s) with whom this data will be shared.	SPS							
b	Directorate(s) or Department(s) responsible for receiving the data.	Local prison.							
c	Roles of staff receiving the data.								
6 a	**Reason(s) for use of the data - (Why)** Description of why the data is required e.g. law, care of individual.	Duty of Care to provide medical support to each prisoner.							
7 a	**Source of data (What system)** Description of the data system(s), from which the data to be exchanged, is obtained.	Information given verbally by prisoner which is subsequently captured and stored in the NHS GP IT systems.				Manual Health Care Record. Paper ACT Record			
b	Description of the module or fields accessed when using another organisation's IT system to share data.	PR2 (SPS Prisoner Records Database)							
8 a	**Form title and reference number - (What form)** The title and reference number of any form or letter used to convey and / or collect the data.	N/A							
9 a	**Destination record(s) / system(s) - (Where to)** The data system(s), record(s) or other destination of the data shared.	PR2 (SPS Prisoner Records Database) modules that deal with Integrated Case Management, Sentence Management, Community Integration Plan, Liberation Scroll, prisoner appointments, activities, tribunals, HDC, service provider referrals, prisoner referrals, BCPs, ACT, risk and conditions, complaint history, generic searches, Operations,							

		height and weight							
10 a	**When exchanged / shared (When)** Details of when the data needs to be exchanged / shared e.g. daily, weekly, monthly, yearly, as and when.	Daily		Weekly		Daily		Weekly	
		Monthly		Yearly		Monthly		Yearly	
		When required	X			When required	x		
11 a	**Communication media (How)** Details of all formats in which the data is to be transferred to the recipient e.g. direct feed from system, verbal transfer at team meeting, telephone call, e-mail.	Telephone		Fax		Telephone		Fax	
		Face to face		Email		Face to face		Email	
		Direct feed from IT system		Access to paper record		Direct feed from IT system		Access to paper record	x
		Access to IT system	X	Copy of paper record		Access to IT system		Copy of paper record	
		Letter or similar				Letter or similar			
12 a	**Communication media controls (How)** Details of how all security controls are applied, e.g. password protected files, encryption of files, including any risks assessments undertaken.	Password protected access. Access based on User Roles.							
13	**Issues or comments not included in the above**								

ANNEX C – DETAILS OF DATASETS AND DATA FLOWS (contd.)

	Description	Data Exchange 4	Data Exchange 5
1 a	**High Level Function(s)** General description of the function(s) or service(s) to which the data relates.	Sentence Management, Warrant information, ACT history	Transfer of Health Care Records and ACT Documentation accompanying prisoner on transfer to another prison.
2 a	**What data will be shared** Description of the data to be provided.		Health Care Record, ACT Record
3	**Personal Identifiers included in the above** Main identifiers being used to identify the individual.	Surname X, First Name X Date of Birth X, Address Prisoner No X, Post code CHI	Surname X, First Name X Date of Birth X, Address X Prisoner No X, Post code X CHI X
4 a	**Provider organisation(s) - (Who from)** Provider organisation(s).	SPS	Health Board
b	Directorate(s) or department(s) responsible for providing the data.	Local prison	Health Board
c	Roles of staff responsible for providing the data.	Criminal Desk	Prison Health Centre staff
5 a	**Destination organisation(s) - (Who to)** Recipient organisation(s) with whom this data will be shared.	Health Boards	SPS (Escort Provider)
b	Directorate(s) or Department(s) responsible for receiving the data.	Health Boards	Partnership and Commissioning Directorate
c	Roles of staff receiving the data.		
6 a	**Reason(s) for use of the data - (Why)** Description of why the data is required e.g. law, care of individual.	Duty of Care to provide medical support to each prisoner.	Duty of care to ensure effective health care provision upon transfer to another Establishment
7 a	**Source of data (What system)** Description of the data system(s), from which the data to be exchanged, is obtained.		Manual Health Care Record. Paper ACT Record.
b	Description of the module or fields accessed when using another organisation's IT system to share data.	PR2 (SPS Prisoner Records Database)	
8 a	**Form title and reference number - (What form)** The title and reference number of any form or letter used to convey and / or collect the data.		
9 a	**Destination record(s) / system(s) - (Where to)** The data system(s), record(s) or other destination of the data shared.		
10 a	**When exchanged / shared (When)** Details of when the data needs to be exchanged / shared e.g. daily, weekly, monthly, yearly, as and when.	Daily, Weekly Monthly, Yearly When required X	Daily X, Weekly Monthly, Yearly When required
11 a	**Communication media (How)** Details of all formats in which the data is to be transferred to the recipient e.g. direct feed from system, verbal transfer at team meeting, telephone call, e-mail.	Telephone, Fax Face to face, Email Direct feed from IT system, Access to paper record X Access to IT system X, Copy of paper record X Letter or similar	Telephone, Fax Face to face, Email Direct feed from IT system, Access to paper record X Access to IT system X, Copy of paper record X Letter or similar
12 a	**Communication media controls (How)** Details of how all security controls are applied, e.g. password protected files, encryption of files, including any risks assessments undertaken.	Paper copies accompany prisoner on transfer to hospital in sealed bag	Sealed in a bag.

13	**Issues or comments not included in the above**		

ANNEX C – DETAILS OF DATASETS AND DATA FLOWS (contd.)

	Description	Data Exchange 6
1 a	**High Level Function(s)** General description of the function(s) or service(s) to which the data relates.	Prisoners under escort from a prison (health information).
2 a	**What data will be shared** Description of the data to be provided.	Prisoner Escort Record
3	**Personal Identifiers included in the above** Main identifiers being used to identify the individual.	Surname X First Name X Date of Birth X Address Prisoner No X Post code CHI
4 a	**Provider organisation(s) - (Who from)** Provider organisation(s).	Health Board
b	Directorate(s) or department(s) responsible for providing the data.	Health Board
c	Roles of staff responsible for providing the data.	Prison Health Centre staff
5 a	**Destination organisation(s) - (Who to)** Recipient organisation(s) with whom this data will be shared.	SPS (Escort Provider)
b	Directorate(s) or Department(s) responsible for receiving the data.	Partnership and Commissioning Directorate
c	Roles of staff receiving the data.	
6 a	**Reason(s) for use of the data - (Why)** Description of why the data is required e.g. law, care of individual.	Duty of Care to ensure effective health care across partner agencies.
7 a	**Source of data (What system)** Description of the data system(s), from which the data to be exchanged, is obtained.	Manual Health Care Records. Electronic Health Care Records (EMIS/Vision)
b	Description of the module or fields accessed when using another organisation's IT system to share data.	
8 a	**Form title and reference number - (What form)** The title and reference number of any form or letter used to convey and / or collect the data.	
9 a	**Destination record(s) / system(s) - (Where to)** The data system(s), record(s) or other destination of the data shared.	
10 a	**When exchanged / shared (When)** Details of when the data needs to be exchanged / shared e.g. daily, weekly, monthly, yearly, as and when.	Daily X Weekly Monthly Yearly When required Other
11 a	**Communication media (How)** Details of all formats in which the data is to be transferred to the recipient e.g. direct feed from system, verbal transfer at team meeting, telephone call, e-mail.	Telephone Fax Face to face Email Direct feed from IT system Access to paper record X Access to IT system Copy of paper record Letter or similar Other
12 a	**Communication media controls (How)** Details of how all security controls are applied,	Prisoner Escort Record (PER) Document

	e.g. password protected files, encryption of files, including any risks assessments undertaken.	
13	**Issues or comments not included in the above**	

Scottish Accord on the Sharing of Personal Information – List of Acronyms

ACT2Care	**SPS Suicide Risk Management Strategy**
CD	**Compact Disk**
CEL	**Chief Executive Letter**
CHI	**Community Health Index**
GPMS	**Government Protective Marking Scheme**
HRIS	**Health Information Rights Scotland**
ICM	**Integrated Case Management**
ISP	**Information Sharing Protocol**
KPI	**Key Performance Indicator**
MOU	**Memorandum of Understanding**
NHS	**National Health Service**
PID	**Person Identifiable Data**
PR2	**Prisoner Records Management System**
SPIN	**Scottish Prison Information Network**
SPS	**Scottish Prison Service**