



Information Sharing Agreement Between

**NHS Ayrshire & Arran
and
East Ayrshire Council
North Ayrshire Council
South Ayrshire Council
and
East Ayrshire Integration Joint Board
North Ayrshire Integration Joint Board
South Ayrshire Integration Joint Board**

Version:	02.1	Supersedes:	02.0	Status:	Approved
Author:	Information Governance Pan-Ayrshire Group	Date Approved:			24/11/2021
Approved by:	Information Governance Pan-Ayrshire Group	Review Date:			24/11/2024

Document uncontrolled when printed

Document Control Sheet

Title:	Ayrshire Information Sharing Agreement
Document Status:	FINAL
Document Type:	Information Sharing Agreement
Version Number:	V02.1
Document location:	Websites internal/external of the parties
Author:	Information Governance Pan-Ayrshire Group (IGPAG)
Owner:	IGPAG
Approved By:	IGPAG
Date Effective From:	24/11/2021
Review Frequency:	Every 3 years or sooner if required
Next Review Date:	24/11/2024

Revision History:

Version:	Date:	Summary of Changes:	Responsible Officer:
02.0	12/12/2018	Updated in line with GDPR & DPA 2018	IGPAG
02.1	24/11/2021	Inclusion of child fair processing requirements, update of security requirement, update of responsible officers	IGPAG

Approvals: this document was formally approved by:

Name & Title / Group:	Date:	Version:
IGPAG	12/12/2018	02.0
Strategic Planning & Operational Group (SPOG)	18/03/2019	02.0
Sign-off from CEO's NHS A&A, EAC, NAC & SAC	-	02.0
IGPAG	24/11/2021	02.1
Sign-off from CEO's NHS A&A, EAC, NAC & SAC		02.1

Dissemination Arrangements:

Intended audience:	Method:	Date:	Version:

Linked Documentation:

Document Title:	Document File Path:

NB. This document is uncontrolled when printed. The contents of this document are subject to change, any paper copy is only valid on the day of printing. To ensure you have the most up to date version of this document please use the link to access the document directly from AthenA or contact the Author.

Contents

Click on the headings below to link to the relevant section.

1.0	Introduction	4
2.0	Legal Framework	4
3.0	Consent	5
4.0	Data Subjects	6
5.0	Information being shared	6
6.0	Purposes of information sharing	6
7.0	Transparency	7
8.0	Information standards	7
9.0	Retention of information	7
10.0	Security of shared information	8
11.0	Subject Access Requests	9
12.0	Information Breach Management	9
13.0	Complaints	10
14.0	Review	10
15.0	Appendix 1 Parties to the Information Sharing Agreement	10
16.0	Appendix 2 General Terms	11
17.0	Appendix 3 Lawful basis	12
18.0	Appendix 3 Information being shared	13
19.0	Appendix 4 Fair processing requirements	14
20.0	Appendix 6 Signatories	16

1.0 Introduction

This Information Sharing Agreement (ISA) has been prepared to support the regular sharing of information between:

- NHS Ayrshire & Arran
- East Ayrshire Council
- North Ayrshire Council
- South Ayrshire Council
- East Ayrshire Integration Joint Board
- North Ayrshire Integration Joint Board
- South Ayrshire Integration Joint Board

Hereafter referred to as the “parties”. Appendix 1 details the party’s headquarters.

The aim of this ISA is to:

- Facilitate the sharing of information between the parties;
- Put in place a framework which will allow this information to be exchanged in ways which respect the rights and freedoms of individuals and in compliance with the law.

This ISA has been developed by the Information Governance Pan- Ayrshire Group.

2.0 Legal Framework

The parties are established and function under the following legislation:

- Local Government (Scotland) Act 2003
- National Health Service (Scotland) Act 1978
- Public Bodies (Joint Working) (Scotland) Act 2014

Disclosure of information will be conducted within the legal framework consisting of:

- Data Protection Act 2018 (DPA)
- UK General Data Protection Regulation
- Human Rights Act 1998

And in compliance with the common law duty of confidentiality

Current data protection legislation requires personal information to be processed in line with the following principles:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate relevant and limited to what is necessary
- Accurate and where necessary kept up to date
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed
- Processed in a manner that ensures appropriate security of the personal data

Service specific legislation including but not limited to:

- Child and Young People (Scotland) Act 2014
- Social Work (Scotland) Act 1968
- Housing (Scotland) Act 2001
- Education (Scotland) Acts 1980 & 2016
- Adult Support & Protection (Scotland) Act 2007
- Anti Social Behaviour etc. (Scotland) Act 2004
- Health (Tobacco, Nicotine etc and Care) (Scotland) Act 2016

The lawful bases for processing personal and special categories of personal data are set out in Data Protection Legislation detailed in Appendix 2.

Most common legal bases for sharing personal data are:

- Processing is necessary for compliance with a legal obligation to which the party is subject
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the party

Most common legal bases for sharing special categories of personal data are:

- Processing is necessary for reasons of substantial public interest
- Processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment, or the management of health or social care systems or services

All information sharing must be justifiable and have an appropriate lawful basis.

3.0 Consent

In limited circumstances where the processing is outwith a statutory duty or public task the information sharing may require an individual's consent as the lawful basis.

Where consent is the lawful basis for processing it must meet the requirements of Data Protection Legislation.

If consent is the lawful basis for processing it must be:

- Freely given
- Unambiguous
- Informed
- Specific
- Verifiable
- Regularly reviewed

Where the parties are relying on an individual's consent as the lawful basis to process personal data individuals have the right to withdraw this consent at anytime.

4.0 Data Subjects

“Data Subject” means the identified or identifiable living individual to whom personal data relates.

- Users of services provided by the parties
- Users of services provided on behalf of the parties
- Users of services of integrated health and social care provided by the parties
- Employees of the parties

5.0 Information being shared

Information will be shared fairly and lawfully and should be restricted to the minimum amount of personal information necessary to achieve the purpose(s).

Information will be shared by the parties in ways which respects the rights and freedoms of individuals and in compliance with the law. Only proportionate, relevant and appropriate information should be shared on a need to know basis.

The following types of data will be shared:

Personal data: any information relating to an identified or identifiable person

Special categories of personal data: any information relating to an identified or identifiable person revealing:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data
- Health data
- Sex orientation
- Personal data relating to criminal convictions and offences

Data being shared under this ISA is detailed in Appendix 3.

6.0 Purposes of information sharing

Information is shared by the parties for the following purposes:

- to enable each Party to discharge its statutory duties and public tasks
- to protect adults and children at risk of harm
- to provide staff with the information they need to deliver joined-up and integrated services
- to produce consistent services and information
- to support joint care planning and commissioning
- to support a single point of access and out of hours services for the community

- to support national initiatives on multi-agency working and information exchange
- to support statutory reporting functions and effective use of resources
- to assist the management teams of the parties with planning and management information

Other purposes which may emerge from time to time provided the parties agree that such further uses are necessary and proportionate and that the information exchange underpinning such purposes is consistent with the over-arching principles of this ISA.

7.0 Transparency

It is necessary to communicate to individuals about how their personal data is processed. Fair processing requirements are detailed in Appendix 4.

All parties will clearly inform individuals in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Where the processing is addressed to a child all parties will communicate fair processing information in a clear and plain language that a child can easily understand.

Agreed methods of providing this information include:

- Verbal and written communication
- Leaflets
- Posters
- Appropriate wording on forms
- Public facing websites

8.0 Information standards

The parties have a responsibility to check the quality and accuracy of the personal data which they hold, with particular emphasis on checking the accuracy and quality of information to be shared.

The parties will undertake to notify the other as soon as practicable if an error is discovered in information which has been provided to the other parties or if changes are made to the personal data e.g. demographic information, to ensure that the Parties are then able to correct or update their respective records.

9.0 Retention of information

The Parties are subject to the Public Records (Scotland) Act 2011, which requires all parties to have an approved Records Management Plan.

All parties must have a records retention schedule. For some records the retention period is laid down by law for other records the parties determine the retention period themselves.

The parties agree that when information has reached the point where it is no longer required by one party, that that party will delete or destroy the information (in accordance with each party's records retention schedule) rather than returning it to the other party.

10.0 Security of shared information

All parties are responsible for the actions of their staff in terms of the processing of information under this agreement. Each party must determine their internal processes necessary to ensure that staff are suitably qualified and trained in terms of the processing of the information under this agreement.

Such internal processes shall include, but are not limited to:

- relevant security checks,
- relevant background checks; and
- relevant qualification checks.

All parties must ensure that they have adequate mechanisms in place to deal with the physical and organisational security of the information.

All parties will ensure that there is a formal process in place to ensure that all information security breaches relating to the information shared under this agreement are reported to the other affected party or parties within a 24 hour period.

With regard to the transfer of data, this will be undertaken by:

Secure Email Transfer

- Email must be secured to ensure the protection of information in transit. This will require encryption to be applied which is at least a comparable standard to FIPS140-2 or 128/256 bit AES encryption;
- Where both parties have been accredited to the National CyberSecurity Centre Secure Email Blueprint (SEB) approved sharing may be undertaken using mandatory TLS rather than using SEB;
- Parties may provide a secure email system which will require the other parties to register before taking receipt of the information.

Secure File Transfer (SFTP)

- Any FTP services must utilise SFTP and therefore encryption. SFTP services must be managed to ensure good practise including: the deactivation or removal of the anonymous account, full management of files stores to ensure short retention periods, management of access to file stores.

Peripherals - Data in Transit

- Data in transit must be encrypted to levels not subject to known flaws or security issues. Encryption in use must be maintained to latest patching and security levels. Data in transit includes that located on smart devices, USB storage devices, optical media etc.

Internet - Data in Transit

- Legacy protocols such as SSL, TLS 1.0 and 1.1 are not permitted, 1.3 is advised. All internet bound traffic must utilize the latest version of protocols available.

Malicious Code Scanning

- All information transferred electronically will be scanned to ensure that no malicious code is passed. The other party will be notified of any virus or malicious infection on the other party's system that could impact the provision of information.

All parties storage and archive areas will have at the very minimum access controls to secure the area and prevent unauthorised entry, have environmental controls and fire and smoke suppression equipment and alarms.

Information when held on office located PC or transient equipment such as laptops and USB devices that does not conform fully to the point above, must be protected by encryption that is at least a comparable standard to FIPS140-2 or 128/256 bit AES encryption.

All parties will ensure information is regularly backed up to ensure the confidentiality and safety of the information.

All parties will ensure they have documented processes in place to ensure the secure destruction of personal information when it is no longer required for its purpose(s).

11.0 Subject Access Requests

Requests for access to personal information will be processed and responded to using the standard Subject Access Request procedure within each party.

12.0 Information Breach Management

Each party will each ensure that the other party is notified of any information security breach, or significant information security risks, affecting shared information within 24 hours.

In compliance with Data Protection legislation the responsible party's Data Protection Officer will assess and consider requirements to report the information breach to the Information Commissioner's Office (ICO).

The parties will, where appropriate, work together to rectify any such information breach or mitigate any such risk to information security, including notification to affected individuals if required.

13.0 Complaints

Each party has a complaints handling procedure by which individuals can direct complaints regarding the services they have received

Complaints relating to data protection concerns can be directed to each party's Data Protection Officer, details are listed in Appendix 1.

14.0 Review

This ISA will be reviewed every three years by the Information Governance Pan-Ayrshire Group or sooner if appropriate.

15.0 Appendix 1 Parties to the Information Sharing Agreement

This document is a binding agreement between:

East Ayrshire Council

East Ayrshire Council Headquarters, London Road, Kilmarnock, KA3 7BU

Chief Executive: Eddie Fraser

Data Protection Officer: Robert Gibson

Telephone: 01563 576094

Email: information.governance@east-ayrshire.gov.uk

East Ayrshire Integration Joint Board

East Ayrshire Council Headquarters, London Road, Kilmarnock, KA3 7BU

Chief Officer: Craig McArthur

North Ayrshire Council

North Ayrshire Council Headquarters, Cunninghame House, Irvine, KA12 8EE

Chief Executive: Craig Hatton

Data Protection Officer: Lauren Lewis

Telephone: 01294 310039

Email: dataprotectionofficer@north-ayrshire.gov.uk

North Ayrshire Integration Joint Board

North Ayrshire Council Headquarters, Cunninghame House, Irvine, KA12 8EE.

Chief Officer: Caroline Cameron

South Ayrshire Council

South Ayrshire Council Headquarters, County Buildings, Wellington Square, KA7 1DR

Chief Executive: Eileen Howat

Data Protection Officer: Wynne Carlaw

Telephone: 01292 612061

Email: DataProtection@south-ayrshire.gov.uk

South Ayrshire Integration Joint Board

South Ayrshire Council Headquarters, County Buildings, Wellington Square, KA7 1DR.

Chief Officer: Tim Eltringham

NHS Ayrshire & Arran

Eglinton House, Dalmellington House, Ayr, KA6 6AB

Chief Executive: Professor Hazel Borland

Data Protection Officer: Jillian Neilson, Head of Information Governance & DPO

Telephone: 01563 825831

Email: InformationGovernance@aacpt.scot.nhs.uk

16.0 Appendix 2 General Terms

In addition to those defined terms set out elsewhere in the Agreement, the following definitions and rules of interpretation apply in this Agreement.

Agreement: means the front end agreement together with these General Terms and Conditions and any annexes attached and signed as relative hereto;

Data Controller: has the meaning set out in the Data Protection Legislation.

Data Processor: has the meaning set out in the Data Protection Legislation.

Data Protection Authority: the relevant data protection authority in the territories where the parties to this Agreement are established.

Data Protection Legislation: while they remain in force the UK General Data Protection Regulation (GDPR), Data Protection Act 2018 and any other laws and regulations relating to the processing of personal data and privacy which apply to a party and, if applicable, the guidance and codes of practice issued by the relevant data protection or supervisory authority.

Data Security Breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the Shared Personal Data.

Data Subject: has the meaning set out in the Data Protection Legislation.

Personal Data: has the meaning set out in the Data Protection Legislation.

Processing: has the meaning set out in the Data Protection Legislation.

Shared Personal Data: means the Personal Data and/or Special Category Data (both as defined in the Data Protection Legislation) to be shared between the parties under or in relation to this Agreement.

Subject Access Request: has the same meaning as “Right of access to personal data” in Article 15 of UK GDPR.

17.0 Appendix 3 Lawful basis

Article 6 UK GDPR Lawfulness of processing

- (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- (c) processing is necessary for compliance with a legal obligation to which the controller is subject;
- (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

Article 9 GDPR Processing of special categories of personal data

- (a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
- (b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
- (c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- (d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

- (e) processing relates to personal data which are manifestly made public by the data subject;
- (f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- (g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
- (h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
- (i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
- (j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

18.0 Appendix 3 Information being shared

Information will be shared fairly and lawfully and should be restricted to the minimum amount of personal information necessary to achieve the purpose(s).

Information will be shared by the parties in ways which respects the rights and freedoms of individuals and in compliance with the law. Only proportionate, relevant and appropriate information should be shared on a need to know basis.

Information shared includes, but is not limited to:

- non-personal statistical and financial information derived from personal data
- research data and findings derived from personal data
- standard demographic information about service users and those involved in their care (names, addresses, dates of birth, contact details etc)
- information to support the line management of employees working within integrated services and/or partnership working arrangements
- unique personal identifiers (including Community Health Index (CHI) numbers and Social Care reference numbers and other internal reference numbers)
- the following information in respect of individuals:
 - Health information e.g. physical and mental health and condition, medication, therapeutic interventions

- Social care information e.g. care plans, needs assessment
- Housing information e.g. housing applications, tenancy information, anti-social behaviour information
- Education information e.g. academic records, attendance, guidance and support
- Financial information e.g. benefits, council tax information
- Criminal convictions and offences
- Fraud prevention information
- Employee information e.g. direct employee management information, workforce planning information

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

- Full Name
- Address, Postcode
- Date of Birth
- Partner system identifiers:
 - Community Health Index (CHI) Number
 - Social work number

19.0 Appendix 4 Fair processing requirements

Article 13 GDPR Information to be provided where personal data are collected from the data subject

Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

- (a) the identity and the contact details of the controller and, where applicable, of the controller's representative;
- (b) the contact details of the data protection officer, where applicable;
- (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- (d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;
- (e) the recipients or categories of recipients of the personal data, if any;
- (f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

- (a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

- (b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
- (c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- (d) the right to lodge a complaint with a supervisory authority;
- (e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
- (f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

20.0 Appendix 6 Signatories

Executed for and on behalf of:	NHS Ayrshire & Arran
Signature	
Name (Print)	
Job Title (Print)	
Date of Signature (Print)	
Location	


Executed for and on behalf of:	East Ayrshire Council
Signature	
Name (Print)	
Job Title (Print)	
Date of Signature (Print)	
Location	


Executed for and on behalf of:	East Ayrshire Integration Joint Board
Signature	
Name (Print)	
Job Title (Print)	
Date of Signature (Print)	
Location	

Ayrshire Information Sharing Agreement

Executed for and on behalf of:	North Ayrshire Council
Signature	
Name (Print)	
Job Title (Print)	
Date of Signature (Print)	
Location	

Executed for and on behalf of:	North Ayrshire Integration Joint Board
Signature	
Name (Print)	
Job Title (Print)	
Date of Signature (Print)	
Location	

Executed for and on behalf of:	South Ayrshire Council
Signature	
Name (Print)	Eileen Howat
Job Title (Print)	Chief Executive
Date of Signature (Print)	25 November 2021
Location	Ayr

Executed for and on behalf of:	South Ayrshire Integration Joint Board
Signature	
Name (Print)	Tim Eltringham
Job Title (Print)	Director
Date of Signature (Print)	25/11/2021

Ayrshire Information Sharing Agreement

Location	Ayr
-----------------	-----