INFORMATION SHARING AGREEMENT

[TITLE]

[REFERENCE]

[RELEVANT DATE]

Contents

1 Parties, Scope and Purpose....4
1.1 Name and details of the parties who agree to share information....4
1.2 Business and legislative drivers for sharing data....4
2 Description of the information to be shared....5
3 Description and manner of information sharing....6
3.1 Data flows....6
3.2 How data/information is to be accessed, processed and used....6
3.3 Summary of how decisions are going to be made with regards to the manner of the processing....6
4 Impact assessments and preparatory work....7
5 Privacy information (transparency requirement)....7
6 Accuracy of the information....8
7 Data retention and secure disposal....9
8 The rights of individuals....9
8.1 Subject access request, FOI and data portability....9
8.2 Objection or restriction to processing, rectification and erasure....9
8.3 Rights related to automated decision making, including profiling....10
8.4 Direct Marketing....10
9 Security, risk and impact of the processing....12
9.1 Agreed standards, codes of conduct and certifications....13
10 International transfers of personal data....14
10.1 List of countries where the data will be transferred to (if applicable)....14
10.2 Reasons for transferring personal data outside the UK....14
11 Implementation of the information sharing agreement....15
11.1 Dates when information sharing commences/ends....15

11.2 Training and communications.....15
11.3 Information sharing instructions and security controls.....15
11.4 Non-routine information sharing and exceptional circumstances.....16
11.5 Monitoring, review and continuous improvement.....16
12 Sign-off.....17
13 Appendix 1 List of Work instructions, policies and procedures.....18
14 Appendix 2 Data items and adequacy.....19

Remember to remove all text in green from your final version as these guidance notes are only added to assist you in completing the template.

1 Parties, Scope and Purpose

1.1 Name and details of the parties who agree to share information

Legal name of parties subject to the ISA and Head Office address	Short name of the party	Role in this agreement : Data Controller or Data Processor (*)	ICO Registration

(*) for Data Processor, please identify on behalf of what data controller(s)

For complex agreements where parties may play dual data controller and data processor roles, describe in subsequent paragraphs or bullet points in what circumstances a party will act as a data controller or a data processor and for which subset of data.

1.2 Business and legislative drivers for sharing data.

Describe the key business drivers for this data sharing – e.g. a new piece of legislation that requires the sharing to happen, a recommendation in an official report, etc.

1.2.1 Purpose(s) of the information sharing

Ensure all the purposes for all of the parties in the agreement are identified, and that it's clear what purposes are related with which party.

Indicate how the data controllers will decide upon changes in the purpose(s) of the information sharing	Jointly or independently

The instructions for reaching agreement on changes in the purposes of the information sharing is described in the [Name of the Instructions] listed in Appendix 1 Instructions.

1.2.2 Legal basis for the processing and constraints

(This section should describe fully the legal basis for all the purposes and for all the parties, because parties may have different purposes and differing legal basis for processing the data).

Without detriment of any other legal basis that may be applicable (e.g. criminal investigation, etc.) the following are the core legal basis for each of the parties to process the data in this agreement:

Legal basis	Party

2 Description of the information to be shared

Data category	Data Controller(s)	PD*

(*) PD – refers to Personal Data in the sense given within the EU General Data Protection Regulation (GDPR) and the Data Protection (UK, 2018) Act.

The parties agree this is the minimum amount of data needed to properly fulfil the purposes of this agreement.

Appendix 2 (Data items and adequacy), contains the list of all relevant data items/fields which it has been agreed can be shared under this ISA, indicating the source and the recipients, and any relevant supporting statement for information that may raise questions on data minimisation.

3 Description and manner of information sharing

3.1 Data flows

(add a diagram describing the data flow)

3.2 How data/information is to be accessed, processed and used

Processing (descriptor)	Associated work instructions, policy or procedure (listed in Appendix 1) If applicable

3.3 Summary of how decisions are going to be made with regards to the manner of the processing.

Describe how the data controllers and data processors are going to make decisions (jointly or independently) about the way the data is processed, the security controls (technical or organisational), etc. – this summary must be consistent with whatever is described in any attached or referenced work instructions, policies or procedures listed in the above table.

4 Impact assessments and preparatory work

Describe whether any relevant risk assessment work or due diligence work has taken place by the parties, such as privacy impact assessments, data protection impact assessments or information risk assessment relevant to the data and the processing subject of this agreement.

Describe any protocol agreed between the parties to review and keep this assessment work up to date, and manage any resulting risks. Refer to any relevant policies and procedures.

A Data Protection Impact Assessment (DPIA) is a process to help you identify and minimise the data protection risks of a project.

You must do a DPIA for any processing that is likely to result in a high risk to individuals. This includes some specified types of processing. You can use the ICO screening checklists to help the parties decide when to do a DPIA.

The ICO also recommends to conduct a DPIA for major projects which require the processing of personal data.

NHS Scotland have also developed a tool to triage the risk and the need for DPIAs or further more detailed risk assessments. Other tools can also be used for this purpose. Describe in this section what has been agreed between the parties in this regard and how risk is going to be appropriately escalated and managed.

The parties acknowledge that any actions and countermeasures agreed as part of the Data Protection Impact Assessment reviews must be implemented by the responsible party. Deadlines and follow up to progress on those actions will be established as part of the DPIA review process.

5 Privacy information (transparency requirement)

Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR.

You must provide individuals with information including: your purposes for processing their personal data, your retention periods for that personal data, and who it will be shared with. The ICO calls this 'privacy information'.

Describe how the data subjects have been informed of this processing, how to exert their data protections rights, etc (check on the ICO website for further privacy notices also known as "Fair Processing Notices"). It is recommended that any specific ICO fair processing notices be referenced in this agreement.

The information provided must be concise, transparent, intelligible, easily accessible, and it must use clear and plain language. Any privacy notices about the processing of health data must be referenced, linked or uploaded via the NHS Inform website in the section "How the NHS handles your personal data"). This approach is in line with the ICO recommendation (layered approach). Other parties may decide to implement alternative ways to communicate with the public.

Further information is available in the ICO website (GDPR, Right to be informed) and their corresponding guidance.

Please identify the relevant Privacy Notices available and where to find them.

Ensure a list of relevant Privacy Information available, such as Privacy Notices and Fair Processing Notice(s) is included in this section and where to find them (e.g. online links).

6 Accuracy of the information

Please describe any arrangements to ensure the accuracy of the data shared and any work instructions or underpinning policies or procedures that may be applicable. Ensure these documents are listed in the Appendix 1 list.

Also describe any arrangements to ensure either the parties or the individual can challenge the accuracy of information, how this request will be managed, by whom and how, this will be updated if appropriate. Work instructions, underpinning policies or procedures may be applicable, if so, ensure these documents are added to the Appendix 1 list.

Remember to remove all text in green from your final version as these guidance notes are only added to assist you in completing the template.

7 Data retention and secure disposal

Describe any agreed arrangements to ensure the data is disposed of when no longer needed – describe retention policies that are applicable to each of the partner organisations.

Describe the length of retention making reference to the appropriate record retention policies which have been agreed between each partner organisation. Consider the purpose or purposes for holding the information when agreeing whether (and for how long) to retain it;

Describe the agreed acceptable methods for securely deleting information that is no longer needed for this purpose or these purposes. If a work instruction, or local policy or procedure exists, please make a reference to it as appropriate.

8 The rights of individuals

Describe in the sections below (8.1 to 8.4) what arrangements will be in place, agreed or independently implemented by the parties with regards to the rights of data subjects under the applicable legislation, e.g. Data Protection Act and Freedom of Information Act]. Feel free to split this section into sub-sections or combine them in a single section if it is easier. The aim is to describe the arrangements the parties have made to ensure every single right of the individual can be exercised.

Consider drafting work instructions if there is a need to link different parties existing processes in order to support a "joint" or linked approach. Create a list in Appendix 1, detailing any work instructions, policies or procedures both new or existing across the parties in support of this obligation.

8.1 Subject access request, FOI and data portability.

Describe how the parties with handle subject access requests, FOIs and data portability requests (if applicable).

8.2 Objection or restriction to processing, rectification and erasure.

Describe how the parties with handle objections or restrictions to processing, request for data rectification and erasure (right to be forgotten – if applicable).

8.3 *Rights related to automated decision making, including profiling.*

[ ] Automated decisions are involved in this agreement – in the context of this agreement, "Automated decisions" refer to decisions made using shared information **with no human** intervention.

[ ] Profiling (automated processing of personal data to evaluate certain things about an individual) is involved in this agreement.

Description

Describe if there are automated decisions (making a decision solely by automated means without any human involvement), including profiling (automated processing of personal data to evaluate certain things about an individual), and if so how the parties plan to comply with the additional rules (GDPR Art. 22), such as introducing simple ways to request human intervention or challenge an automated decision. This type of processing has direct impact on explicit consent, therefore, regardless of the preliminary legal basis, the parties may need to reconsider the need for consent at this stage. Remember to mention any work instruction, policy or procedure, new or existing across the parties in support of this obligation, which should be listed in Appendix 1.

At this point in time, the parties may agree that there is no automated decision making or profiling, however, in the event of future changes requiring automated decisions, the parties can agree now how they would wish to deal with this change.

For example they may scrutinise and approve or agree to carry out or update the DPIA to consider and address the risks before they start any new automated decision-making or profiling. This may include telling the public about the profiling or automated decision-making being proposed, who's going to approve it (jointly or independently), or perhaps agree on using anonymised data for any profiling activities, etc. (as per ICO best practice recommendations).

8.4 Direct Marketing

The GDPR gives individuals the right to object at any time to processing of their personal data for the purposes of direct marketing. The right to object to marketing is absolute and you must stop processing for these purposes when someone objects. There are examples for opt-in/opt-out in the ICO Direct Marketing Guidance.

The GDPR gives a specific right to withdraw consent. You need to tell people about their right to withdraw, and offer them easy ways to withdraw consent at any time.

It has long been the view of the ICO that anything that seeks to promote goods or services, whether they be free or charged for, falls within the definition of marketing for the purposes of the Privacy & Electronic Communications Regulations 2003 (PECR), when carried out via email, telephone or text (i.e. electronic communication).

For example, a patient who has provided their mobile telephone number and who has arranged an appointment with a GP Practice, may be sent a text reminder because they have initiated the arrangement and the reminder is specific to that arrangement.

Invitations via electronic media to take up 'Flu vaccination, health reviews, etc., where prior consent has not been obtained, are not initiated by the patient but by the Practice and would be considered to be promotional activity on the part of the Practice. As such, by far the best way to proceed with this will be for Practices to have a discussion with patients as and when they are seen to ascertain their amenability to receive promotional communications and to record their consent to demonstrate compliance.

While invitations for vaccinations or health reviews would appear prima facia to be benign, we have had cause previously to take a Health Board to task on the same grounds for a proposal to send text invitations to attend sexual health clinics which could be seen as intrusive. Moreover, while many people will undoubtedly be grateful to be offered support in promoting and protecting their health, or who may be more broadly interested in the promotion of public health ideals, there will always be individuals who do not. For example, promoting vaccination to someone who has a strong inclination against vaccinations would likely find such communication most unwelcome.

Keeping this in mind, the parties should consider if as part of the processing related to this agreement they aim to use Direct Marketing, and if so, what are the agreed mechanisms to ensure compliance and how the opt in/out mechanism will be implemented.

In the ICO Direct Marketing guidance, you will find options for approaching customers and offering an opt out. The parties must consider the proportionality of this approach (e.g. invitations to vaccinations to patients at high risk) and to offer a suitable opt out. This should be documented in the DPIA and any residual risk accepted by the parties SIROs accordingly.

[ ] Direct marketing is involved in this agreement

Description

Describe is this section any arrangements to manage Direct Marketing. Rather than repeating, you can just refer to specific work instructions, policies or procedures attached in Appendix 1 if they are fit for reflecting the governance arrangements around direct marketing agreed by the parties.

9 Security, risk and impact of the processing

[ ] All relevant Security Policies applicable to the parties and systems used in this proposal are available and listed in Appendix 1.

[ ] A qualified Information Security Officer has reviewed the adequacy of the attached Security Policies and has advised on the technical and organisational security risk level.

[ ] A suitable process to document and monitor the security risk described in the Information Security and Governance Policies listed in Appendix 1.

[ ] A Data Protection Impact assessment has been produced and is available as listed in Appendix 1.

[ ] A competent, independent and free of conflicts of interests Data Protection Officer has been designated to inform the Data Controllers on the adequacy of this agreement and the corresponding compliance and any residual risks documented in the Data Protection Impact Assessment.

[ ] A Data Protection Impact assessment has been produced and is available as listed in Appendix 1.

The security measures put in place across the parties ensure that:

[ ] Wherever special categories of data are processed, the data will be encrypted at rest and in transit.

[ ] Wherever special categories of data are transmitted over network, Transport Layer Security (TLS) protocols will be applied. Exceptions will

be documented in the DPIA and any residual risk will require approval by the SIRO of each organisation prior to processing such data.

[ ] only authorised individuals can access, alter, disclose or destroy data. This is achieved through the following work instructions, policies and procedures (also listed in Appendix 1):

In the bullet points below, list any relevant policies/procedures that explain the arrangements between the parties for these controls.

-

[ ] authorised individuals act only within the scope of their authority. This is achieved through the following work instructions, policies and procedures (also listed in Appendix 1):

In the bullet points below, list any relevant policies/procedures that explain the arrangements between the parties for these controls.

[ ] if personal data is accidentally lost, altered or destroyed, it can be recovered to prevent any damage or distress to the individuals concerned. This is achieved through the following work instructions, policies and procedures (also listed in Appendix 1):

In the bullet points below, list any relevant policies/procedures that explain the arrangements between the parties for these controls.

-

The security controls applicable by each organisation will be:		Jointly agreed between the parties
		Independently decided by each party

9.1 Agreed standards, codes of conduct and certifications

In the bullet points below, list any specific agreed standards, codes of conduct or certification the parties have agreed to adhere by as part of this agreement e.g. ISO 27001, Cyber Essentials, etc.

-

10 International transfers of personal data

Personal data shared in line with this agreement will be transferred to:

With regards to the information shared under this agreement, indicate the list of countries where the parties have agreed the data can be transferred to outside the UK – and describe the basis for adequacy of the protection level for the rights and freedoms of data subjects in relation to the processing of shared personal data. Refer to the current list of such countries on the European Commission's data protection website. Consider if the processing involves subcontracting services which may involve transferring data abroad (e.g. data backups, cloud services, web based systems in which data servers are hosted abroad, etc.)

	EEA countries only
	Out with EEA
	Will not be transferred outside the UK

10.1 List of countries where the data will be transferred to (if applicable).

List the countries in the bullet point below or describe which areas are involved and how. (e.g. Latin-America). If there are no international data transfers, delete this section (sub-section 10.1).

-

10.2 Reasons for transferring personal data outside the UK.

If there are no international data transfers, delete this section (sub-section 10.2).

-

11 Implementation of the information sharing agreement

11.1 Dates when information sharing commences/ends

11.2 Training and communications

Describe what steps have been put in place to train staff involved with the processing of the data in this agreement and, if necessary, communications to data subjects and publishing information about this processing in websites etc.

11.3 Information sharing instructions and security controls

There is no need to add anything in this section, but confirm the parties acknowledge their obligations to follow the work instructions, policies and procedures in Appendix 1.

You may also want to use this section to outline any security classifications (e.g. OFFICIAL SENSITIVE) that are relevant to the information being shared and confirm that the security controls are adequate.

All relevant information sharing instructions, including but not exclusively any work instructions, policies or procedures, are listed in Appendix 1 and accepted by all parties.

The applicable security classification for the data in this agreement are as follows:

-

11.4 Non-routine information sharing and exceptional circumstances

Use this section to describe, what the parties plan to do in circumstances where there is a request or need to share information related to this agreement but either slightly out of scope (e.g. more data items than the ones initially identified) or under

different legal basis or circumstances (e.g. international transfers to countries initially not listed etc.). For example, 'the parties will never share any information which is out-with the agreed scope of the ISA" or, 'the parties will escalate to a designated manager for approval', or 'the parties will have freedom to decide in circumstances where there is no material time for wider consultation, in order to protect the physical and mental health of a person' – this section should aim to agree in advance how to approach the governance around exceptions that may come up.

11.5 Monitoring, review and continuous improvement

Describe when this ISA needs to be reviewed (i.e. at least annually), how the parties aim to monitor progress and performance of this agreement, and how the parties can trigger a review/update of this ISA or any of the underpinning work instructions, the DPIA, transparency/privacy notices etc.

Describe if there is any particular group to be created for these purposes and its membership (ideally it is recommended to add and refer to the corresponding group role and remit in Appendix 1).

12 Sign-off

"We the undersigned agree to the details recorded in this Information Sharing Agreement; are satisfied that our representatives have carried out the preparatory work set out in the Information Sharing Tool-kit for Scotland and are committed to the ongoing monitoring and review of the scope, purpose and manner of the information sharing."

[Copy as many of these boxes as needed depending on the number of signatories – at least one per party]

Name of the Party		
Authorised signatory	Title and name	
	Role	
Signature and date		
Data Protection Officer		
Senior Information Risk Owner		

Name of the Party		
Authorised signatory	Title and name	
	Role	
Signature and date		
Data Protection Officer		
Senior Information Risk Owner		

13 Appendix 1 List of Work instructions, policies and procedures

Work instructions title	Organisation	Where to find this document (e.g. hyperlink)

14 Appendix 2 Data items and adequacy

Data Item	Source	Recipients	Data minimisation justification	For data linkage only

Remember to remove all text in green from your final version as these guidance notes are only added to assist you in completing the template.