INSTRUCTIONS

The Scottish Information Sharing Toolkit (IS Toolkit) is an evolution of the former SASPI (Scottish Accord on the Sharing or Personal Information 2011) and the former Gold Standard in the direction of minimising personal and non-personal information risks across organisations.

The Toolkit has been in use since 2016 and was made mandatory for NHS Scotland wherever NHS health data was shared in 2017.

This version has been reviewed in line with GPDR and the new Data Protection Act (2018).

GENERAL GUIDANCE:

A. How to use the ISA template

All main sections are required (headed in bold and numbered 1. 2. 3. and so on), however sub-sections may be aggregated and combined in a paragraph as long as the topic is dealt and not avoided. All sections in the template deal with a regulatory requirement, therefore all should be considered.

By aggregating sub-sections, the template can provide some flexibility to adapt to a variety of scenarios, however all topics must be considered during the negotiations of an ISA, otherwise there will be no assurance that all relevant GDPR and DPA 2018 requirements have been considered.

B. Who should sign off the ISA

Due to the nature of this agreement, the recommendation is that Senior Information Risk Owners (SIROs) sign off these agreements and DPOs should be involved throughout the approval process to inform the SIRO.

SIROs may delegate this responsibility to other responsible managers and Information Asset Owners.

For National agreements, the Public Benefit and Privacy Panel (PBPP) may approve and sign agreements on behalf of the health boards in NHS Scotland, since they have delegated powers, however other parties may need to be approached via alternative routes as required.

For ISAs approved by this method it is sufficient to provide the application reference number and the date of the PBPP approval letter. No additional signature is required to represent the NHS Scotland health boards, but other parties may still need to countersign.

In this case, the recommendation is to complete the signature on behalf of the Health Boards following this example:

Name of the Party		NHS Scotland
Authorised signatory	Title and name	Public Benefit and Privacy Panel
	Role	On behalf of NHS Scotland Health Boards
Signature and date		Application number: X12345 approved: 01/01/2018
Data Protection Officer		Mini Mouse

Senior Information Risk Owner	IG pack sent to all SIROs at Health Boards

This method can be followed by other groups as long as the parties involved have conferred sufficient delegated powers to the approval body acting as signatory.

C. How to produce the ISA ? Who should be involved?

An Information Sharing Agreement is a result of a negotiation process, therefore it should be approached as the outcome of a process rather than a paper exercise.

The recommendation is to ensure that people with a good understanding of the data flows and the business requirements drive the process assisted by a Data Protection Officer, Information Security Officer, Caldicott Guardians, Legal Office and relevant professional bodies as required, depending on the complexity of the agreement.

Since the Information Sharing Agreement is between Data Controllers, it is obvious all data controller should participate – no party can make decisions another party unless there are relevant delegation powers in place. For example, a group of GPs may decide to nominate someone else (it could be a professional body, but other options could also apply) to represent their interests in the agreement. This representation may include only the preparation work and discussions or may include the actual sign off, depending on the level of powers delegated.

From experience with cross public sector data sharing, it is best to start drafting from the business need perspective (services driving the sharing) with the advice of a Data Protection Officer or Information Governance expert, and involve subsequently specific advisors as needed e.g. (Information Security Officer, etc.).

Once a draft DPA is prepared, it is recommended to consult other relevant groups, professional bodies and legal office before sign off.

The ISA should be a document that clarifies the agreements and practicalities around the sharing, it should use clear language that is helpful for information governance purposes and for practitioners who have to implement what has been agreed, however it is expected to contain a degree of information governance / data protection terminology.

The language of work instructions, policies and procedures should be easily understood by those who have to follow them.

D. When to draft an ISA ?

ISAs are recommended whenever regular/systematic data sharing between two or more parties needs to occur.

Although ISAs are not a legal requirement, this is best practice (ref. ICO Data Sharing Code of Practice). Since 2017, NHS Scotland Health Boards are required to complete an ISA for any systematic information sharing where NHS Scotland's data in processed.

This will generally involve routine sharing of data sets between organisations for an agreed purpose. It could also involve a group of organisations making an arrangement to 'pool' their data for specific purposes.

E. Should organisations publish their ISAs?

ISAs in the context of the public sector are documents subject to Freedom of Information, therefore the parties are welcome to publish ISAs as they would do with any other policies, procedures and privacy notices. Prior to publishing ISAs, the parties should establish if there is any perceived security risk the organisation may be exposed to by publishing specific sections or appendixes of the agreement, such as diagrams. If a security risk exists then these portions should be withheld.

F. Where can I get further information or training on using the IS Toolkit ?

Your Data Protection Officer or Information Governance team should be able to provide assistance in first instance.

G. Headers and footers

Remember to update the short title in the header of the page, and add a short reference number to the document.

This must also be added to the front page.

In the footer, insert the relevant date – this is the date the agreement should **start.**

Example of **title for main page**:

- Provision of NHS Scotland data for the Breast and Cosmetic Implant Registry (BCIR)

Example of **short title** for header:

- NHS Scotland - BCIR

Example of **reference**:

- BCIR-ISA2018

H. Removing guidance text from final version

I. General advice

REMEMBER

If you are using the template with the "quick green prompts", then remember to remove all the green guidance text from your final version as this is only added for your assistance.

Please check the spelling and formatting of the completed template and update the contents page by right clicking on it and the selecting *update field* and then *update the entire table.*

J. Further assistance

For further information contact:

Information Assurance Team,
Digital Health and Care,
Scottish Government
St. Andrews House,
Regent Road
Edinburgh
EH1 3DG

Contents

Introduction

Provide an executive summary of this agreement, why it is important and any other key messages that need to be communicated to the readers of this agreement who might not be interested in reading the entire document.

1 Parties, Scope and Purpose

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

Identify all the parties in the agreement, if the head office address is easily found you may omit this information but it is recommended to include it for easy identification of all the parties, especially with smaller organisations.

You may want to generalise some group names, e.g. a negotiation between NHS Digital (England) for sharing data with all health boards in Scotland, should list all the relevant boards (because some special boards may not be included) in one cell of the table and in the “Short Name” row, add NHS Scotland. If there is a leading board in the negotiation you may want to add that board the first on your main list in bold with an explanatory note at the bottom of the table.

Since the ICO is changing the register after 25th of May 2018, you may decide that is not the right time to add ICO registration numbers. This is acceptable at the moment.

If some parties are going to play a dual role or you have a combination of data controllers and data processors, it is important to be clear what role(s) each party is playing in this agreement.

ISAs can be used also to supplement data processor agreements or commercial agreements and SLAs with subcontractors where there is a component as a data processor, along with other parties who play a data controller role. To simplify the need for multiple agreements (data processor and information sharing), the ISA could be used for this dual purpose. In any case, the role of the parties must be clear in this section.

For complex agreements where parties may play dual data controller and data processor roles, describe in subsequent paragraphs below the table (or in bullet points) in what circumstances a party acts as a data controller or a data processor and for what subset of data.

Example:

Legal name of parties to ISA	Short name of the party / Data Controller status	Head Office address
NHS DIGITAL	NHSD (Data controller)	1 Trevelyan Square, Leeds LS1 6AE
NHS National Services Scotland*	NSS (Data processor)	Gyle Square 1 South Gyle Crescent Edinburgh EH12 9EB
NHS National Services Scotland* NHS Ayrshire and Arran* NHS Borders* NHS Dumfries and Galloway* NHS Fife* NHS Forth Valley* NHS Grampian* NHS Greater Glasgow and Clyde* NHS Highland* NHS Lanarkshire* NHS Lothian* NHS Orkney* NHS Shetland* NHS Tayside* NHS Western Isles* NHS National Waiting Times Centre* (The Golden Jubilee)	NHS Scotland (Data controller)	

(*) all the parties except NHSD are collectively referred to as "NHS Scotland" in this document. NHS Scotland has delegated decision powers to PBPP (Public Benefit and Privacy Panel) to scrutinise and authorise the sharing on their behalf.

NSS will act as data processor on behalf of the rest of the NHS Scotland during the recall of implants process (data flow attached). NSS will act as data controller for any other activities in this agreement (e.g. initial data feeds from NSS datasets to BCIR).

In this example, since there is a need for NSS to be mentioned for specific tasks that are different to the rest of the health boards, we decided it was convenient to keep a short name for them and also clarify they may act as part of NHS Scotland or as NSS (data processor) in the agreement. In this example the particular role of NSS was clarified later in the document.

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.

In a few sentences, describe broadly what this information sharing aims to achieve without getting into too much detail.

Insert the circumstances which have led to the parties deciding that they need to formally share (or share more information); you may want to cite any examples of negative impacts that occurred because of lack of information sharing in the past and any information which needs to be shared to satisfy legislative changes.

It is always good practice to describe the benefits of the proposed sharing from the organisation and people/public's perspective as applicable.

Example:

The Department of Health directed NHS Digital to carry out this work in response to Recommendation 21 of the Keogh Review of the Regulation of Cosmetic Interventions.

See link:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192028/Review_of_the_Regulation_of_Cosmetic_Interventions.pdf

NHS Scotland would also like to join the Registry. Data will be needed to help run this effectively so in the event of an implant recall, patients can be contacted using their up-to-date contact information. The main benefit/aim of joining the Registry is to reduce the burden on NHS Scotland should an implant recall be generated in the future (as with the PIP health scare in 2010).

1.2.1 Purpose(s) of the information sharing

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

Example:

NHS Digital has developed a Breast and Cosmetic Implant Registry (BCIR) which captures the details of breast implant procedures completed in England by both the NHS and private providers.

The registry is operational in England and was launched on 10 October 2016. This agreement includes the sharing of data covering Scotland so similar data to England can be shared for the Registry to function effectively. This is for the purpose of patient safety so patients can be contacted at up-to-date addresses should there be an implant recall in the future.

NHS Digital may publish reports on the total numbers and types of implants, procedures and outcomes. These reports will only contain aggregated information (that is, data that has been grouped or combined) so that no individual patient will be identifiable.

Purpose description	Primary / secondary purpose
The primary purpose of the BCIR is to record the details of any patient, who has had breast implant surgery, so that they can be traced in the event of a product recall or other safety concern relating to a specific type of implant. Should an implant recall arise, an agreed process will be followed.	Primary
The secondary purpose of the BCIR is to provide an 'early warning system'. A later phase of the registry is to consider a facility to enter anonymised data, especially if this remains a consented registry for England. This would then help provide a denominator for the total number of implant procedures, so if there was to be a recall in the future, the registry would indicate the full scale of the recall. More data on the registry would better inform an outlier process through the identification of any trends and complications related to specific implants	Secondary

Indicate how the data controllers will decide upon changes in the purposes of the sharing	Jointly or independently
	Changes in the purposes of the data will be decided jointly.

The instructions for reaching agreement on changes in the purposes of the sharing is described in the Data Access and Information Sharing Policy listed in Appendix 1 Instructions.

NHS Scotland are the data controllers for these data items but once the data has been shared with NHS Digital and patient details updated onto the Registry, it is expected that NHS Digital and the rest of data controllers identified as NHS Scotland will become data controllers in common for these data items.

1.2.2 Legal basis for the processing and constraints

Ensure the legal basis for all the purposes and all the parties are included, as parties may have different purposes and differing legal basis for processing the data.

Example:

Without prejudice of any other legal basis, including more specific or exceptions in the law (e.g. crime prevention), the main legal basis for the core purposes on this agreement is the National Health Services (Scotland) Act 1978 (c29) (general duties of Scottish Ministers to provide a health service and to promote the improvement of the health of the people of Scotland). In addition, the Data Protection (2018) Act and the new General Data Protection Regulations (GDPR 2018) are:

If sharing personal data according to Data Protection Act 2018 and GDPR 2018	
Core legal basis for processing personal data	Core legal basis for processing special categories of personal data
• GDPR Art. 6 1(d) - Vital interest of the data subject • GDPR Art. 6 1(e) – public task / task in the public interest (NHS functions)	• GDPR Art. 9 2 (c) - vital interest • GDPR Art. 9 2 (g) – substantial public interest • GDPR Art. 9 2 (h) - provision of health or social care or treatment by professionals under "secrecy" obligations such us duty of confidentiality - Art. 9 (3) • GDPR Art. 9 2 (i) public health (includes medical products and devices – such as cosmetic implants) and • GDPR Art. 9 2 (j) – archiving, research and statistical purposes

2 Description of the information to be shared

Outline in bullet form the clear categories or fields of data/information that are agreed to be shared including any personal identifiers; indicating clearly which party is the owner (and if relevant Data Controller of that data). There is no need to discuss data flows at this point. Then complete Appendix 2 – Data items/fields list and confirm the Data Controller status for the shared data.

Example:

NHS Digital shall provide NSS with a list of patients that need to be traced. On a routine basis, NSS will provide the relevant CHI numbers. Only at the point of an implant recall will patient address and postcode be provided.

Data category	Data Controller status	Personal Identifiable Data (*)
Basic patient demographics (patient unique identifier and address), details about the surgeon and NHS Board where implant took place	At source: NHS Scotland Once shared: NHS Scotland and NHS Digital (as described in section 1.3)	Y (Sensitive)

Note: The following paragraphs in the template are mandatory and should not be removed:

"The parties agree this is the minimum amount of data needed to properly fulfil the purposes of this agreement. Failure to process these data items can have a significant detrimental impact on data subjects in the event of a recall.

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

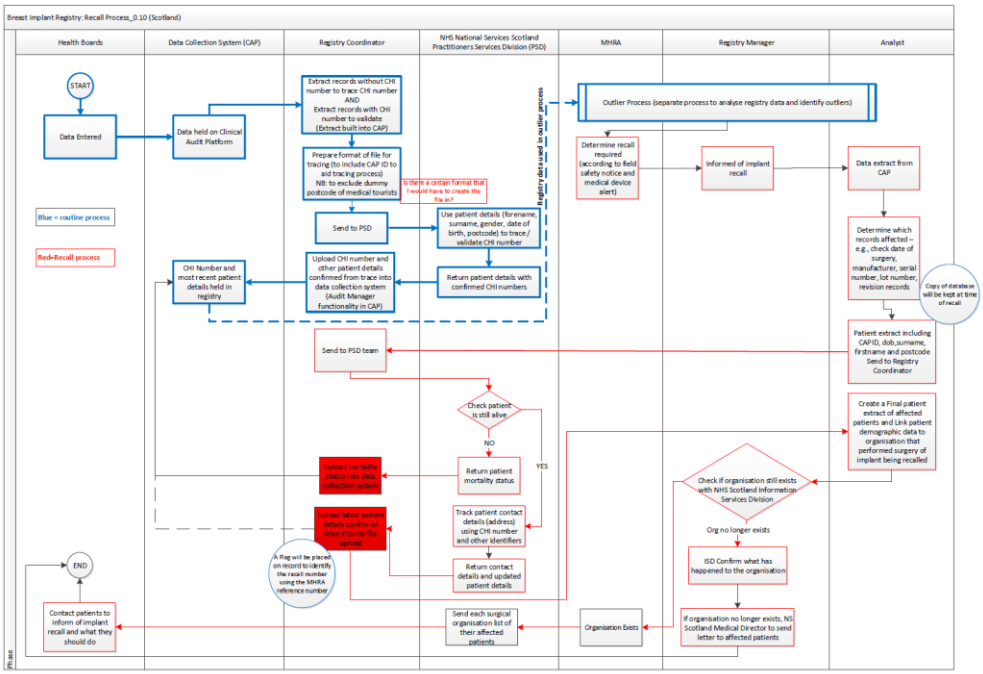
Preferably add a diagram describing the data flow or refer to an appendix with the diagram. Alternatively a narrative description of the data flow can be included or bullet points. A data flow must identify clearly:

- Sources and recipients (e.g. organisation and system)
- Data Categories including an indication of what data is personal identifiable data, anonymised or pseudo anonymised
- What happens in the destination (briefly)

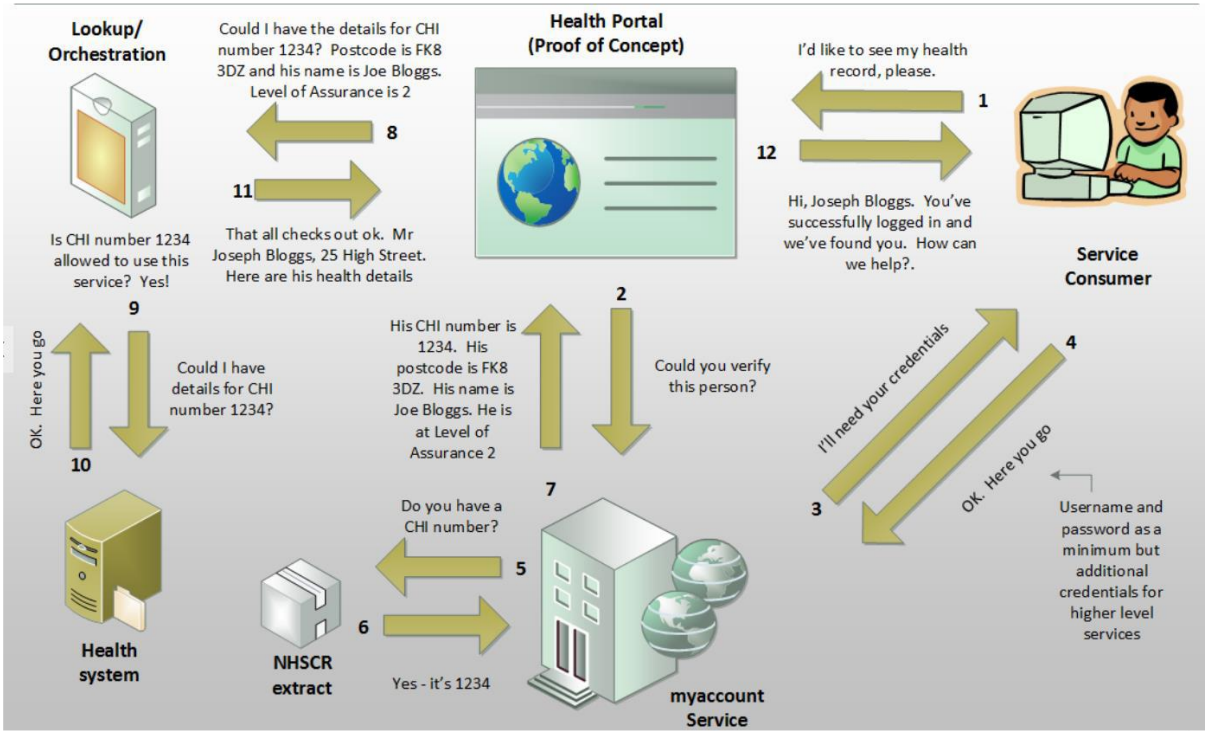
All sources and destinations must be identified, therefore the level of detail should be balanced. A too high level diagram will not describe sufficiently what's happening with the data. A too detailed diagram may be overwhelming and difficult to read, therefore a reasonable balance should be sought.

Below there are some examples for illustration purposes only, the actual data flows may differ as they are regularly reviewed as part of the relevant projects activities.

a) Recall data flow for Breast Implant Registry (2018)

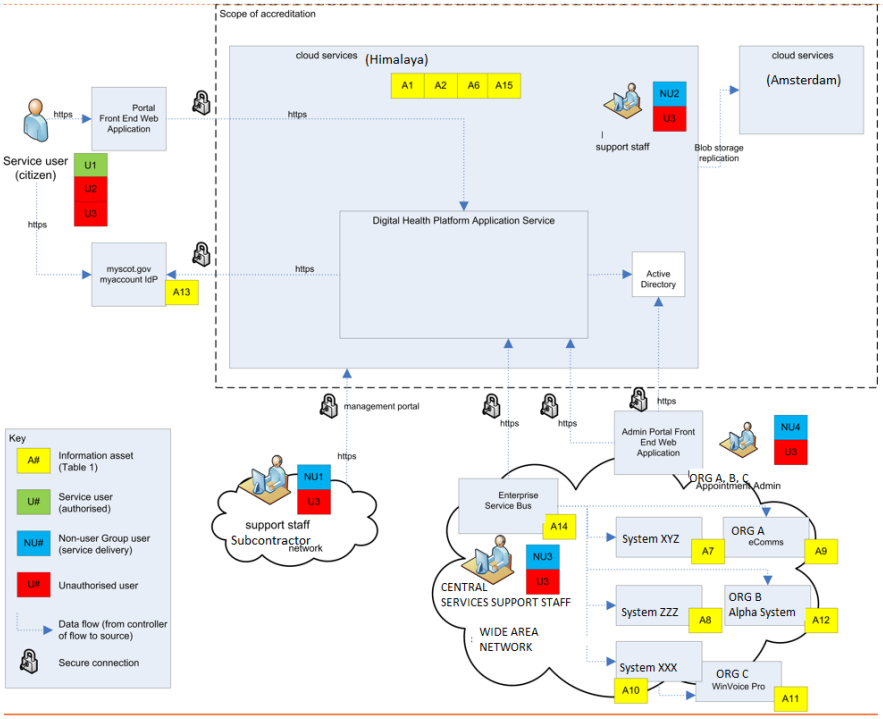


b) Citizen/Patient sign-in proof of concept data flow example.



c) Digital service platform (adapted illustrative example from a national platform).

For the following example to be considered a data flow diagram, it should include at least a legend indicating the data categories flowing through the diagram. Therefore, an illustration like this will not be sufficient in an ISA. If all data categories could potentially flow through any point on the diagram, it would be sufficient to indicate this in a legend.



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

Insert in bullet form how each party will then use the data/information received from another party as a result of the information flow. Note: it is important to consider if the purpose and manner may change once the information has flowed from its originating organisation to another organisation. It also needs to be clear how far parties' are providing:

- access to view data (i.e. exposing it)
- are using messaging technology to send an image of it
- are extracting copy data and transferring it or physically (e.g. in case of manual files) sharing original data/information
- or is there any further sharing expected with other organisations beyond the parties subject to this agreement.

Describe the circumstances in which the data will be used.

Example:

Data use description	Associated work instructions, policy or procedure (listed in Appendix 1) If applicable
The CHI number will be updated/inputted into the Clinical Audit Platform so information is complete for patient records.	See Recall Process flow diagram
The patient address and postcode information will be updated (if applicable) on the Clinical Audit Platform so providers can then view the updates and send recall letters to any affected patients.	See Recall Process flow diagram

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.

Example

Changes in the manner of the processing will be decided jointly except for security measures (organisational or technical) of local nature (e.g. local network settings etc.) which will be decided independently (e.g. it is reasonable to expect that for practical

reasons NHS Digital will not search for joint approval with NHS Scotland for changes in the security controls of their ICT infrastructure or the BCIR/CAP system).

The instructions for reaching agreement on changes, in the manner of the sharing is described in the policies listed in Appendix 1 (Instructions), particularly in the Data Access and Information Sharing Policy.

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 assessments 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 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 organisations to conduct a DPIA for major projects which require the processing of personal data.

NHS Scotland has also developed a tool to triage the risk and the need for DPIAs or 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.

Example:

Please refer to the most up to date version of the Data Protection Impact Assessment Document.

The initial DPIA has been reviewed by NSS, Scottish Government, the Public Benefit and Privacy Panel (Scotland) and NHS Digital prior to this agreement. Where the hazard log referenced privacy statements, this work refers.

The Scottish Government will provide a coordinating role to ensure the data processing and events are reviewed annually and information is fed back to the NHS Scotland Boards Information Asset Owners (IAOs) and Data Protection Officers (DPOs).

Subsequently, NHSD will review and update the DPIA on regular basis, as part of their information governance processes and:

a) will escalate to Scottish Government and NHS Scotland (NSS) any major risks derived from the processing of the data. NSS will coordinate communication/escalation to NHS Scotland boards via local Data Protection Officers and SIROs.

b) will search for agreement with NHS Scotland for any changes in purposes and any non-local matters related with the processing that may involve organisational or technical measures for which NHS Scotland will become data controller, including those related to processes to accommodate data subject's rights and/or decisions over international transfers.

c) once a year NHD will provide an information assurance report to the Scottish Government and NHS Scotland (NSS) including a summary of data breaches, the current risks position and an up to date DPIA for the BCIR. NHS Scotland (NSS) will share these reports with the NHS Scotland Data Protection Officers, IG Leads, Caldicott Guardians and Siro's prior to the preparation of their annual information assurance statement.

The following paragraph is mandatory and should not be removed from the template:

Mandatory Statement: 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 stablished as part of the DPIA review process.

Impact on people interests

Agreed arrangements to minimise the impact of the sharing of information on the interests of the people concerned both as a group and individually.

Example:

Overall, sharing this information is the public interest; specially in cases of an implant recall, when it could be of vital interest for the individual.

Appropriate controls to minimise unnecessary privacy impact are described in the DPIA and include data minimisation, data access controls, encryption, security of the system, etc.

A further analysis is available in the DPIA. The parties agree to review and keep the DPIA up to date as controls and risks may change overtime. The Information Asset Owner at NHSD, NSS and NHSScotland are responsible for reviewing and updating the DPIA accordingly on regular basis. Refer to section 12.5 for further reviewing and monitoring arrangements.

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 protection rights, etc , Refer to the ICO website for further guidance on privacy notices also known as "Fair Processing Notices".

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 for a layered approach. Other parties may decide to implement alternative ways to communicate with the public.

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

Please identify **all** 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) are included in this section and where to find them (e.g. online links).

Example:

Information is available on the NHS Digital BCIR webpage. Information is also to be provided in a patient information leaflet which is expected to be provided to the patient during their initial consultation by the provider/surgeon.

This information is also signed posted to patients via NHS Inform, "How the NHS handles your information" section.

NHS Scotland has considered the benefits and risks for patients, and determined not sharing this information will be detrimental for the interest of patients in case of a recall and in some cases could have serious adverse consequences to their vital interests. The NHS Scotland withholds a liability to identify and notify individuals in such recall events, therefore the inclusion of NHS Scotland patients in the BCIR is not optional (not subject to opt-out). The patient will be informed of this during initial consultation and it will be explicit in the fair processing notice and on NHS Inform which will host the Scottish patient leaflet and link to the BCIR webpage.

NHS Scotland will not rely on consent for the processing but the legal basis identified in section 1.4 of this agreement.

Posters are also to be displayed in clinics.

List of relevant Fair Processing Notice(s)

- BCIR - Patient Information Leaflet [insert link]
- NHS Digital BCIR web page: http://content.digital.nhs.uk/bcir
- BCIR Poster (source: NHS Digital Communications Team)

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, to 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 Appendix 1 list.

Example:

Agreed steps to ensure the accuracy of any data shared.

Patients will be advised to contact their GP notifying any changes to their basic demographic details (eg name or address). The up to date details will be refreshed in the register at recall time.

For changes on information related to the implant or the procedure, the NHS Board should correct that information directly in the registry entry.

Agreed arrangements for any challenges to the accuracy of information

Patients can exert this right by making a Subject Access Request (SAR) to NHS Digital asking for the information and identifying any changes required.

NHS Digital will validate with the provider (eg an NHS Board in Scotland). Discrepancies will be resolved following the approach described in section 1.1. of this agreement.

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 for each of the partner organisations.

Describe the length of time making reference to the appropriate record retention policies which have been agreed by 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 to securely delete 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 as appropriate.

Example:

This is an ongoing Registry. If for some reason that the Registry was to close down in the future then records would be retained for 5 years after the closure. Records would be retained and disposed of in accordance with the NHS Digital Records Management Procedure: Retention and Disposal schedule.

Data about NHSScotland patients will be transferred to NHSScotland in an electronic standard format agreed between the parties.

See Appendix A (Record type: Clinical Audit data) of the NHS Digital Records Management Procedure: Retention and Disposal schedule.

See Section 9.2 of the NHS Digital Records Management Procedure: Retention and Disposal schedule.

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 all of the data subject's rights can be exercised.

Consider drafting work instructions if there is a need to join processes existing in different parties in order to support a "joint" or linked approach. Any work instruction, policy or procedure, new or existing across the parties in support of this obligation, should be listed in Appendix 1.

In our example, arrangement are sufficiently simple to aggregate most of the rights in a single subsection as follows:

Example:

Subject access request, FOIs, data portability, objection to processing

Refer to processes for Subject access request, FOIs and Objection to processing (Links provided in Appendix 1)

SAR, FOIs and Objection to processing could be presented via any of the data controllers following their own process. The first recipient of such a request could contact the relevant Data Protection Officers in the NHSScotland or NHS Digital to ensure the request is processed throughout the data flow as required by GDPR, triggered by a single request.

Patients will not be asked to submit separate request to each data controller.

The coordinating role in NSS /SG will be the point of contact for Boards to notify if there is a FOI and pass these requests to NHS Digital and vice versa. The contact details will be in the IG Pack given to NHS Boards and shared with NHS Digital.

Data Portability rights are not applicable since the data is not processed under Consent grounds.

Automated decisions are not used in this processing.

Profiling is only used to determine patients who received an implant in the event of a recall.

If the situation requires different sub-section, for example for easiness explaining the arrangement, use the following sections:

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).

Example:

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 a 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 currently there is no automated decision making or profiling, however, in the event of future changes requiring this type of decision, its useful to decide now how the parties want to deal with this (scrutinise and approve etc.), e.g. the parties may agree to carry out or update the DPIA to consider and address the risks before they start any new automated decision-making or profiling, telling the public about the profiling or automated decision-making being carried out, who's going to approve it (jointly or independently), or just 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 the 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 it 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, and are not initiated by the patient but by the Practice and could 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 or inappropriate. 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.

Tick the box in this section if Direct Marketing is involved in this agreement and use the section underneath to describe any arrangements to manage those activities.

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 arrangement around the direct marketing agreed by the parties.

Example:

In the example related to the Breast Cancer Registry, there is no marketing involved. However below you can find an example for invitation to participate in a vaccination programme.

---

[x] Direct marketing is involved in this agreement

Describe:

Vaccination invites sent to patients at high risk. For patients at low risk there the letter indicates how they can opt out (refer to instructions in Appendix 1: Vaccination invite letters).

---

9 Security, risk and impact of the processing

In this section, the parties must ensure all relevant security policies are included in the appendix, and that a qualified Information Security Officer has reviewed these policies etc.

Fill in the checklist and tick the box once the parties are satisfied on completion.

The second section requires ensuring some security controls are in place. Tick the boxes following advice from a qualified Information Security Officer who also may

help listing the relevant policies in Appendix 1 that relate to specific organisational or technical controls.

Example:

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

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

[x] 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.

[x] 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):

- *Data access policy (NHSD) – Appendix 1*
- *Data access policy (NSS) – Appendix 1*
- *Information Security Policy available on each NHS Scotland health board (includes data access protocols) – Not in appendix 1 but available on demand approaching each of the Boards.*

The security controls applicable by each organisation will be:		Jointly agreed between the parties
	x	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.

- *IG Toolkit (England)*
- *ISO27001 (certification not required but working towards – all parties)*

- *Cyber Essentials (NHSD and NSS)*

10 International transfers of personal data

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

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. Review the latest list of such countries on the European Commission's data protection website. Consider if the processing involves subcontracting services which involve transferring data abroad (e.g. data backups, cloud services, web based systems where data servers are hosted abroad, etc.)

If there are international data transfers, tick the corresponding box in the table (EU or out with EEA) and list the countries in the bullet point below or describe what general area the countries belong to (e.g. Latin-America).

If there are no international data transfers, delete this subsection as they are not applicable.

Example:

In our example there are no international transfers.

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

10.2 Reasons for transferring personal data outside the UK.

Delete this sub-section if there is no international transfer of data.

If international data transfers are required, describe the reason and the adequacy decision for each of the countries involved.

11 Implementation of the information sharing agreement

In this section complete the relevant subsections as follows:

11.1 Dates when information sharing commences/ends

11.2 Training and communications

11.3 Information sharing instructions and security controls

11.4 Non-routine information sharing and exceptional circumstances

11.5 Monitoring, review and continuous improvement

- Specify the dates when information sharing commences/ends
- 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.
- Describe any non-routine information sharing and exceptional circumstances. How the parties agree to proceed 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 a 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 is aimed to agree in advance how to approach the governance around exceptions that may come up.
- 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).
- You will also notice that there is a section "Information sharing instructions and security controls". There is no need to add anything in this section, except to 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.

12 Sign-off

Complete the information about the signatories.

There are different options for obtaining the sign off from all parties. The template includes options for:

- A small number of parties engaged in the ISA. The template provides sign-off "boxes" for a couple of parties, however, you can copy and paste as many of these boxes as needed depending on the number of signatories.

If a large number of parties are involved, other formats may be more appropriate. The template provides options for:

- Signing-off the ISA by parties who have delegated powers to a particular body or person to act on their behalf (e.g. Public Benefit and Privacy Panel has powers to approve data sharing on behalf of Health Boards within NHS Scotland).

- Signing-off the ISA by a large number parties who must sign individually.

In these cases, the template provides additional paragraphs that must be added as required, but the text in "green" must be deleted from the final version as it is only to help those drafting the ISA.

A separate template has been included in the Tool-kit (Multi Party Sign Off Form) to be used to collect signatures of a large number of parties (e.g. all GPs opting in to a particular project for which an specific ISA is needed). The Multi Party Sign Off Form can be extended in content as needed in order to cover aspects that may be required.

Example of use:

In the following example GPs may who want to use "Florence" (an app used across health and social care) may use this form to opt in to this particular telehealth/telecare project, request a licence (supplied by the Health Board) and acknowledge the arrangements contained in the information sharing agreement (ISA), therefore the following paragraph was added to the Form:

"By signing this "Opt In Form", the General Practice requests licence from [HEALTH BOARD] to use Florence for the provision of contracted health care services as per GMS Contract 2018.

The use of Florence is undertaken as Joint Controllers with the Health Board, as part of the existent Information Sharing Agreements between the parties, in particular the National ISA NHS-GP that covers the wider information sharing required for the GMS Contract.

The Health Board will subcontract and manage the contract with [NAME OF THE DATA PROCESSOR] on behalf of the Joint Controllers (Health Board and GP)."

In this way, even with a large number of data controllers that need to sign individually at different points in time along the life of the project, they can sign off the ISA in an organic but consistent manner.

13 Appendix 1: List of Work instructions, policies and procedures

Finally ensure all relevant work instructions, policies or procedures agreed between the parties to regulate the processing of the data are included in this appendix.

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

The above table should list all:

- Instructions for reaching agreement on any changes to the purpose of the sharing.
- All applicable and relevant Information Security and Governance Policies
- All Data Protection Impact assessments

14 Appendix 2: Data items and adequacy

Also ensure all data items are listed in appendix 2, the source, the recipients, any necessary justification for why the item is necessary (minimisation justification) and therefore must be shared, and if a data item is used only for data linkage but not required for other purposes.

Data Item	source	recipients	Data minimisation justification	For data linkage only

The above table should contain 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.

If you need further assistance with the IS Toolkit you can find details about who can assist or provide further guidance at the start of this booklet.

Finally remember to check the template's formatting and spelling and update its contents page by right clicking on it and selecting 'update field' then 'update the entire table'.