Cefnogir gan
Lywodraeth Cymru
Supported by
Welsh Government

Wales Accord on the Sharing of Personal Information

Guide on the development of Information Sharing Protocols

For organisations involved in the protection, safety, health, education and social welfare of people in Wales

(including statutory, private and third sector organisations)

Version 5 (2021 update)

Contents

Section 1 – The Development Process

Introduction

1.1 This guidance has been prepared to support the development of **Information Sharing Protocols (ISPs)** under the national framework provided by the Wales Accord on the Sharing of Personal Information (WASPI). This document specifically relates to the ISP template available on the WASPI website – www.waspi.org.

1.2 The principles set out in the Accord are put into practice through a collaborative approach to the development of agreements using WASPI templates. Separate guidance is available on the other types of WASPI agreements.

1.3 ISPs help organisations demonstrate how they meet the requirements of data protection legislation; namely the requirements of 'accountability' and 'data protection by design and default' set out in the UK General Data Protection Regulation (UK GDPR).

1.4 ISPs help organisations to set out, in a consistent and clear manner, the detail of personal information shared for specified purposes to deliver public services. The template and this guidance have been produced by stakeholders from a range of organisations and with the support of Welsh Government and the Information Commissioner's Office.

1.5 ISPs are not a substitute for a culture of collaboration and consultation, which is a crucial part of effective public service delivery. As such, ISPs should be prepared with the input of all partners and should not be drafted in isolation. In order to pass the quality assurance process, collaboration and consultation needs to be evidenced.

Considerations before developing an ISP

1.6 ISPs are not always required. Refer to the WASPI website for guidance on when to use an ISP and when to use a different type of agreement or contract. Before starting the development of an ISP you should be able to answer yes to the following:

Question / consideration	Further guidance / notes
Have you consulted with your Data Protection Officer, Information Governance Lead or equivalent regarding the need for an ISP?	**Prior to starting the development of an ISP, you must take advice from a suitably qualified and/or experienced person.**
Prior to sharing personal information, have you considered the need for and, where required, completed a Data Protection Impact Assessment / Privacy Impact assessment?	Information Commissioner's guidance on DPIAs and Article 35 of the UK GDPR. This should be discussed with your Information Governance department or Data Protection Officer.
Does the information being shared identify individuals?	If data to be shared does not identify individuals, an ISP is not required.
Is information reciprocally shared; ie does it flow between organisations or do organisations each contribute specific pieces of personal information?	ISPs should be developed to document practices involving **the regular, reciprocal sharing** (i.e. information flows back and forth between organisations) of

	personal information between Data Controllers. Data Disclosure Agreements are intended for use when personal data is to be **disclosed** (i.e. passed one way) from one Data Controller to another for a specific purpose. Separate guidance and templates are available on the WASPI website to assist with the DDA development process. This should be discussed with your Information Governance department or Data Protection Officer.
Are all partners to the ISP Data Controllers or are any data processors involved?	Data processing activities must be underpinned by a contract compliant with current Data Protection legislation.

1.7 Data Protection Impact Assessments (DPIA), also known as Privacy Impact Assessments, are a legal requirement in certain circumstances and should be undertaken before sharing takes place. A DPIA allows key risks and mitigations (including the need for an ISP) to be identified.

1.8 Take advice if you are unsure whether an ISP is required; this could be from your Data Protection Officer or other suitably qualified person within your organisation. The central WASPI team can provide general advice.

1.9 ISPs should be developed to document practices involving **the regular, reciprocal sharing** (i.e. information flows back and forth between organisations) of personal information between Data Controllers. Data Disclosure Agreements are intended for use when personal data is to be **disclosed** (i.e. passed one way) from one Data Controller to another for a specific purpose. DDAs are not intended for use in instances where the disclosure is from a Data Controller to a Data Processor and do not replace the requirement for appropriate contracts. Separate guidance and templates are available on the WASPI website to assist with the DDA development process.

1.10 Once it has been decided that an ISP is likely to be required, consideration should be given to the identification of the information sharing partner organisations. ISPs **must** be developed collaboratively.

Preparing to develop an ISP

1.11 All partners should abide by the principles set out in the Accord. This demonstrates a commitment to a consistent approach to sharing personal information. Signing the Accord is not a pre-requisite to sharing information but is strongly recommended. The 'Declaration of Acceptance and Participation' is available on the WASPI website.

1.12 Before beginning ISP development, the ISP author/owner should review the ISP Register on the WASPI website to determine whether there are similar assured ISPs or ISPs under development. Existing ISPs can provide a useful baseline but should never be copied without fully considering their relevance and adapting them as required.

1.13 Relevant contacts at partner organisations should be established and the need for an ISP agreed. Roles and responsibilities during the ISP development process should be agreed at an early stage; eg will representatives of partners meet to discuss the ISP, will there be a mixture of physical meetings and virtual meetings or will the ISP be developed by one organisation and feedback provided by email.

ISP development – roles, responsibilities and process

1.14 One organisation – **the lead organisation** – usually co-ordinates the development of an ISP. Typically, the lead organisation is a large public sector body but this is not always, and does not have to be, the case.

1.15 The lead organisation identifies an **author** to manage the development process and draft the ISP. The author may be supported by other contributors / reviewers as required.

1.16 In addition to drafting the ISP, the author is responsible for ensuring the ISP is signed by each organisation following assurance by the appropriate regional quality assurance group.

1.17 Partner organisations should each nominate a **contact / owner** of the ISP to contribute to the development process and ensure ISPs remain relevant to the services they support.

1.18 It is important that the ISP author and organisational contacts consult with their **Information Governance team / Data Protection Officer** (or equivalent) who can provide specific advice about the need for an ISP, interpretation of data protection legislation and how to meet specific requirements, such as the need to inform individuals how their personal information is used.

1.19 The central **WASPI Team**, based within Digital Health and Care Wales can provide advice regarding the WASPI framework, including the development process, use of templates and the quality assurance process. Final drafts of ISPs should be submitted, with the completed pre-quality assurance checklist (see the ISP template), to the WASPI team (waspiservice@wales.nhs.uk) who will conduct an initial check before liaising with the relevant regional quality assurance group.

1.20 **Regional quality assurance groups** are responsible for quality assuring ISPs developed in their area/region. The aims of the groups are to maintain integrity of the WASPI framework, ensure that ISPs are suitable for sharing as examples of good practice and to confirm that the risks and opportunities associated with information sharing have been appropriately assessed and mitigated. The QA groups will confirm that draft ISPs are suitable to be signed by organisations and published as examples of good practice. QA groups will not provide legal advice – partner organisations are responsible for seeking their own legal advice and assurance. QA groups are about ensuring good practice not legal advice. Alternatively, they will provide feedback to the author on required actions.

1.21 A flow diagram of the ISP Development Process can be found at **Appendix A** of this guide.

Section 2 – Populating the ISP template

Introduction

2.1 This section deals with the population of the ISP template, providing guidance on completion of specific sections.

2.2 The aim of the ISPs are to identify and document:

- the scope and specific purpose(s) of the sharing of personal information;
- the partner organisations involved;
- the lawful basis;
- the information to be shared;
- how service users' rights will be met; and
- the agreed secure information transfer methods and controls to be used.

2.3 The WASPI ISP template, available on the WASPI website, has been pre-populated with standard text and clearly indicates where additional information is to be inserted. **The format and standard wording should not be changed without prior consultation with your information governance team and the central WASPI team where required.**

Pre quality assurance checklist

2.4 The first page of the ISP template is a pre quality assurance checklist, which provides an overview of the details of the ISP. Completion of the checklist provides assurance that key considerations have been taken into account during the development of the ISP. It should only be completed when the final draft has been agreed and is ready to be submitted for quality assurance.

2.5 It is expected that the ISP author will complete the checklist. An ISP will not be accepted for quality assurance without a fully completed checklist.

2.6 The WASPI team will remove the checklist prior to publication but will keep an electronic copy as part of the audit trail of the ISPs development.

2.7 **Section 1 –** insert the 'ISP title'. This should be an appropriate name which reflects the function of the service / initiative / project / programme and the geographical area covered, for example: 'The Flying Start Programme – Torfaen'. This should be replicated on the cover page of the ISP.

2.8 **Section 2 –** provide the name, organisation and contact details of the person(s) completing the ISP – the 'author'. Providing these details enables the WASPI team and/or the QA group to contact the author with any queries.

2.9 **Section 3 –** provide the name, organisation and contact details of the Information Governance lead consulted during the development process. This provides assurance that advice has been sought from an appropriately qualified and/or experienced person.

2.10 **Section 4** – tick the relevant box to indicate whether a Data Protection Impact Assessment / Privacy Impact Assessments (DPIA / PIA) has been undertaken. It is a statutory requirement to undertake a DPIA/PIA in certain circumstances (Article 35 of the UK GDPR). If a DPIA has not been completed, use this section to explain why it was not needed.

2.11 **Section 5** – provide the name and organisation of those consulted during the development process. This provides assurance that there has been an appropriate level of consultation. Organisations consulted should ensure that their Data Protection Officer is aware of the development of the ISP.

2.12 **Section 6** - the ISP Author should clarify:

- In section 6(a) list how many organisations are partners to the ISP.
- In section 6(b) that section two of the ISP has been cross referenced with the Information Reference Table. This has been included based on experience that shows this section is often inconsistent.
- In section 6(c) whether any partner organisations remain non signatories to the Accord. Whilst signing up to WASPI is not a prerequisite to being part of an ISP, it is recommended. The ISP author should contact these organisations to outline the benefits of joining WASPI.

2.13 **Section 7** – changes to that standard, agreed template should not be made without prior consultation with the WASPI team. Where changes have been agreed, they should be set out in this section.

2.14 **Section 8** – Confirm that copies of the fair processing information have been submitted with the ISP. Ensure that reference to these documents is made in the table of Section 6 of the ISP.

Title page

2.15 Provide the ISP title in the first ‘insert details here’ box. It should reflect the function of the service / initiative / project / programme and the geographical area covered, for example: The Flying Start Programme – Torfaen. This should be consistent with section 1 of the pre quality assessment checklist.

2.16 The ISP author should outline whether the ISP being developed is a new ISP or if it is a review of an existing ISP available via the online ISP Register.

2.17 The cover page also contains the date the ISP was assured and identifies the relevant QA group. The WASPI Team will complete this once the ISP has been assured. Details of the QA Groups, including contact details are available on the WASPI website or from the WASPI team.

Section 1 - Introduction to this ISP

2.18 This section has been pre-populated with standard text; however, the following details need to be added, to expand on the scope and purpose of the specific ISP.

2.19 At paragraph **1.3** state the name of the particular service / initiative / project / programme and the geographical area covered, for example: ‘The Flying Start Programme – Torfaen’. This should be consistent with the title page and the pre quality assurance checklist.

2.20 At paragraph **1.4** explain the purpose of information sharing, the function of the service and what it seeks to achieve. This can be taken from your Data Protection Impact Assessment. This explanation should be written in a way that allows someone with no knowledge of the function or service to understand what it is about and why it is necessary to share the information.

Section 2 - The information sharing partner organisations

2.21 Each organisation – whether they are from the public sector, third sector, private sector or other – participating in a service that involves sharing personal information becomes an information sharing partner.

2.22 Only data controllers should be listed in an ISP. Data processing arrangements need to be addressed in a contract.

2.23 In the table at paragraph **2.1,** list:

- The organisations that are involved in the sharing of personal information supported by this ISP.
- The details (should be job role, not name) of the Owner / Point of Contact.
- The Departments / Divisions / Teams typically involved.

2.24 Following quality assurance of the ISP, organisations can use Appendix C to ensure that all partner organisations have signed the ISP. Where the ISP author has added additional appendices, references to appendices through the ISP should be checked and updated.

Section 3 - Specific organisational / practitioner obligations

2.25 This section of the template ISP has been pre-populated with set text therefore, no further population is required. However, partners must ensure they comply with these requirements.

Section 4 - Legislative / statutory powers

2.26 Much of this section of the template is pre-populated but the tables need to be completed.

2.27 Identifying an appropriate lawful basis for sharing information is crucial. Without a clear lawful basis, organisations cannot demonstrate that they meet the first principle of UK GDPR (Article 5); 'lawfulness, fairness and transparency'.

2.28 Because there is the potential for both the UK GDPR and the Data Protection Act 2018 (DPA 2018) to provide the relevant lawful basis for sharing information, it is important that appropriate advice is sought prior to drafting an ISP. A lawful basis should be established prior to entering into any arrangements that involve the regular sharing of information. **This does not prevent information being shared in 'emergency situations' or override any existing safeguarding or other procedures and processes established to ensure individuals can be cared for, treated or otherwise protected.**

2.29 A 'How to use the tables' section has been included to aid understanding of this section. This should be read before attempting to fill out this section. If there remains

queries on this section after reading this and this guidance, you should contact your Information Governance team / Data Protection Officer for advice.

2.30 **The tables** – the legal bases for sharing have paraphrased for the purposes of the template. Full details are available at Article 6, 9 and 10 of the UK GDPR and Chapter 2 of part 2 of the DPA 2018. In the case of sharing for law enforcement purposes by competent authorities, further details are available at part 3 of the DPA 2018. Guidance is available on the Information Commissioner's Office website.

2.31 Typically, only one lawful basis from each table should be selected but there may be instances where separate exchanges within the same service rely on different legal bases. An explanatory note should be provided to clarify where different partners rely on different lawful bases. There is no need to list all partners, eg 'Local Authorities rely on Article xx, Police rely on Article xx'.

2.32 The notes sections of the tables explains the additional information to be provided, which varies depending on the relevant lawful basis. Where prompted to explain or provide detail, this should be completed.

2.33 Some legal basis require an Appropriate Policy Document (APD) to be in place for each organisation involved in the ISP prior to sharing. Where an APD is required, this is referenced in the notes of section 4 of the ISP template. A copy of APD does not need to be submitted with the ISP. The Information Commissioner's Office website provides further guidance on this including a template for use.

Section 5 - Details of personal information being shared

2.34 Only the table setting out the personal identifiers to be used needs to be completed. This is not to be confused with the detail of personal information shared, which is set out in the Information Reference Table.

2.35 The table should outline how data subjects (the service users) will be identified so that partner organisations know they are dealing with the same individual. Do not include any information that identifies individuals here or in any section of the ISP. Also, be mindful that to comply with the principle of 'data minimisation', the personal information shared must be limited to that required for the specific purpose (identifying the individual). Usually, name, address, data of birth and a specific reference number are sufficient to identify an individual but it is for the partners to the ISP to agree what is appropriate.

Section 6 – Data subjects' rights

2.36 Allowing data subjects to exercise their rights is an important part of complying with data protection legislation.

2.37 Much of this section is pre-populated but there is a focus on the 'right to be informed' (Article 12-14 of the UK GDPR), which itself is a core element of the principle of 'lawfulness, fairness and transparency'.

2.38 Data protection legislation does not specify the medium through which the informing activity should take place but sets out what should be included and when it should be provided.

2.39 Given the significance placed on this right by the legislation, the table in this section asks each partner organisation to specify how data subjects are informed about how

their information is used. Methods of informing data subjects must be established before a service goes live and the table must be populated with specific information, including the document title and method of delivering information to data subjects.

2.40 Organisations are encouraged to add electronic versions of any leaflets and forms available in the appendices.

2.41 Further advice on individual rights is available via the Information Commissioner's Office website.

Section 7 - Information security

2.42 This section of the template ISP has been pre-populated with set text therefore, no further population is required. However, partners must ensure they comply with these requirements.

Section 8 – Review, Breaches and Termination of this Agreement

2.43 ISPs should be reviewed every two years or sooner if significant changes to the service are made. This will ensure ISPs remain relevant.

2.44 Examples of scenarios that trigger a review:

- 2 years passed since the ISP was assured.
- Significant changes to the scope of the service leading to the involvement of numerous new partner organisations.
- Significant changes to the scope of the service varying the volume or type of personal information being shared.
- A significant (ie reportable) data breach.
- A change to the lawful basis for sharing information.

2.45 Examples of scenarios that do not necessarily trigger a review:

- A new partner organisation is involved in service delivery. If this introduces any of the scenarios highlighted above a review should be considered. It is important to keep an audit of communications that confirm new partners are aware of the terms of ISP, and to complete due diligence on the security of personal data, but new organisations can be added as part of the regular review process.
- The author or any organisational contact leaves post. This will not impact on the validity of the ISP. However, if the ISP author leaves their post, the lead organisation should ensure that someone else takes on this role to ensure the agreement is kept up to date.

2.46 Where an organisation has breached the terms of an agreement, it should be reported to the Owners / Contact Points in Section 2. All organisations party to the agreement should be informed and discuss the implications and next steps. This may result in the organisation being omitted from the agreement or the information sharing set out in this agreement ceasing.

2.47 Where information sharing ends, the Partners involved in the agreement should agree the roles and responsibilities, including whether the information will be deleted

or returned. Please inform the Central WASPI Team who will update the ISP Register.

Appendix A – Glossary of terms

2.48 A glossary defines common references. This can be added to if required but items should not usually be deleted.

Appendix B – Information Reference Table

2.49 This section provides guidance on populating the Information Reference Table (IRT), which is where the detail of information sharing and the associated controls is recorded.

2.50 Insert the name of the ISP at the top of the page. This should be consistent with the title page.

2.51 **At the top of each column**, label the significant information exchanges that support the service. 'Referral', 'Assessment', Allocation', 'Intervention' are commonly used labels but they must be relevant to the specific service. Please add/remove columns where applicable. The WASPI website hosts an Excel version of the Information Reference Table, which can be used where there are more than four information exchanges. Where the Excel copy is used, the table should be removed and a copy of the Excel document should be embedded.

2.52 **Row 1** requires a brief description of the process or stage to which the information exchange relates. Each significant exchange of information must be recorded in a separate column. Note that the purpose of the ISP and the IRT is not to capture every possible exchange of information but the significant information exchanges required to deliver the service.

2.53 **Row 2** requires the detail of the personal information exchanged at each stage to be listed. You are not required to go into 'field level' detail and can categorise the type of information shared. As data controllers, each organisation is responsible for ensuring the information shared is adequate, relevant and limited to what is required to meet the specific purpose of each stage. This row sets out the type of information typically shared. Also, be mindful that to comply with the principle of 'data minimisation', the personal information shared must be limited to that required for the specific purpose.

2.54 **Row 3** requires details of the provider and recipient partner organisations together with the teams typically responsible sending / receiving the information. As data controllers, each partner organisation is responsible for ensuring personal data is accessible only to those individuals who need it as part of their role.

2.55 **Row 4** requires details of the specific technical and organisational controls and safeguards in place to protect the personal information shared. These controls must be organisationally relevant; ie not all controls will be applicable to all partners. The purpose of this section of the IRT is to:

- Ensure appropriate consideration has been given to the security of personal information.
- Demonstrate compliance with data protection legislation – namely paragraph 1 of Article 24 of UK GDPR.

- Provide partner organisations with confidence to share personal information.

2.56 **Row 5** asks whether consent is being relied on as the lawful basis for sharing. The legislation sets a high bar for consent and there are additional implications (eg individuals must be able to withdraw their consent). As such, it is important to identify and consider information exchanges that do rely on consent to confirm that it is appropriately relied upon.

2.57 **Row 6** provides additional notes for practitioners. Completion of this row is optional.

Appendix C – Partner Organisations Signatures

2.58 Following assurance of an ISP you will receive a communication from either the central WASPI team or the relevant quality assurance group informing you of the result of the discussion at the regional quality assurance group.

2.59 The ISP should be signed by each partner organisation. Accepting the ISP by signing it is a key element of principle of 'accountability'. The ISP author is responsible for obtaining the signatures for partner organisations.

2.60 All partner organisations should be listed in Appendix C of the template and it is for partners to determine how to manage the signatory process; ie whether 'does the hard copy of the ISP need physically signing or are electronic signatures are sufficient.

2.61 The signatory should be an individual person with authority to sign the ISP on behalf of the organisation. Check with your Information Governance department or Data Protection Officer if you are unsure who should sign.

2.62 Once signed by all partners, notify the WASPI team (waspiservice@wales.nhs.uk), to enable them to update the register. You will not need to provide a copy, notification will suffice.

Appendix A – ISP Development Flow Diagram