



## Wales Accord on the Sharing of Personal Information

# Information Sharing Protocol for Intermediate Care Team – Pembrokeshire

**Version** Final – V1

Date Assured 21<sup>st</sup> January 2021

Quality Assurance Group Mid & West Wales WASPI QA Group

## Contents

1	Introduction to this ISP	2
2.	The information sharing partner organisations	2
3.	Specific organisational / practitioner obligations	3
4.	Legislative / statutory powers	3
5.	Personal information to be shared	7
6.	Data Subjects' Rights	7
7.	Information security	8
8.	Review of this ISP	9
9.	Appendix A – Glossary of Terms	10
10.	Appendix B – Information Reference Table for the Intermediate Care Team – Pembrokeshire	12
11.	Appendix C – Partner Organisations Signatures	15
12.	Appendix D – WAST Data Disclosure Agreement	15

## 1 Introduction to this ISP

- 1.1 This Information Sharing Protocol (ISP) is supplementary to the Wales Accord on the Sharing of Personal Information (WASPI) and has been agreed following consultation between the participating partner organisations.
- 1.2 This ISP is intended to help practitioners understand what information can be shared between the listed partners for the stated purpose(s). It also provides assurance that the partners have considered the requirements of data protection legislation.
- 1.3 This ISP has been prepared to support the regular sharing of personal information for the intermediate care team in Pembrokeshire.
- 1.4 Personal information is shared for the purpose of implementing a joint team for a more integrated approach between Health, social and third sector services in the delivery of intermediate care by working together to improve how individual's needs are met to prevent an admission to hospital unnecessarily or support a timely transfer back home. The vision for the service is a single point of contact and a dedicated intermediate care team of professionals solely involved within the teams function and not working in other acute or community settings.

## 2. The information sharing partner organisations

- 2.1 The table below sets out the organisational partners to the ISP, the key contact points and the departments, divisions and teams typically involved in sharing information for the purposes described in this ISP.

Information Sharing Partner Organisations	Owner / Point of contact	Departments / Divisions / Teams
Pembrokeshire County Council	Head of Service	Social Services – Adult Care & Housing
Hywel Dda University Health Board	General Manager	Community and Primary Care
Pembrokeshire Association of Voluntary Services (PAVS)	Chief Officer	PIVOT

- 2.2 The ISP owners / points of contact have overall responsibility for this ISP within their respective organisations and must therefore ensure the ISP is disseminated, understood and acted upon by relevant practitioners.
- 2.3 The owners / point of contact for each partner organisation will regularly monitor and review the use of this ISP to ensure information is shared effectively and appropriately.
- 2.4 Once the ISP has been assured, each partner organisation will nominate a signatory to sign the ISP at Appendix C. The signatory will be an appropriate person from the partner organisation who can sign on behalf of the organisation.
- 2.5 Whilst not a signatory partner organisation to this ISP, the Welsh Ambulance Service Trust (WAST) will make referrals into the service subject to standalone Data Disclosure Agreement (DDA) which is attached as Appendix D.

---

### 3. Specific organisational / practitioner obligations

- 3.1 Any breaches of security, confidentiality and other violations of this ISP must be reported in line with each partner organisation's incident reporting procedures. Consideration should be given to sharing the outcome of any investigation, where appropriate, with other partners to the ISP.
- 3.2 Practitioners who share information in line with this ISP should make themselves aware of, and adhere to, their organisation's Information Governance and records management procedures; in particular the provisions that relate to collecting, processing and disclosing personal information.
- 3.3 Every reasonable step should be taken to ensure that inaccurate personal data are erased or rectified without delay. Consideration must be given to advising partner organisations that they may have received inaccurate information. In circumstances where partner organisations cannot be informed, advice should be taken from an Information Governance lead (or equivalent).

### 4. Legislative / statutory powers

**STAFF SHOULD NOT HESITATE TO SHARE PERSONAL INFORMATION IN ORDER TO PREVENT ABUSE OR SERIOUS HARM, IN AN EMERGENCY OR IN LIFE-OR-DEATH SITUATIONS.**

**IF THERE ARE CONCERNS RELATING TO CHILD OR ADULT PROTECTION ISSUES, THE RELEVANT ORGANISATIONAL PROCEDURES MUST BE FOLLOWED**

- 4.1 The sharing arrangements described in this ISP takes into account the relevant data protection legislation, the Human Rights Act 1998 and the common law duty of confidence.
- 4.2 Before sharing personal information, partner organisations must have identified a clear legal basis for doing so.
- 4.3 Data protection legislation includes the concept of:
  - **'personal data'**; any information relating to an identified or identifiable (living) natural person, and
  - **'special categories of data' / 'sensitive processing'**; personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation

Whilst information about deceased people is not covered by data protection legislation, data about deceased people is covered by a similar level of confidence.

- 4.4 Further information and guidance on lawful processing of personal information can be found on the Information Commissioner's website; [www.ico.org.uk](http://www.ico.org.uk)

- 
- 4.5 Partner organisations also need to ensure they take into account the Data Protection Act 2018 and any additional requirements it places on the use of the legal bases set out in Articles 6, 9 and 10 of GDPR (see Part 2 of the Act) and processing for the 'law enforcement purposes' (see Part 3 of the Act). The ICO has guidance on this matter and queries about the relevance of any legal basis should be raised with an Information Governance lead.
- 4.6 Consent to process personal data should not be confused with consent to receive the service. The two are separate and should not be confused or merged.

### HOW TO USE THE TABLES

The following tables are designed to allow partners to this agreement to highlight the lawful bases relevant to the sharing described in this ISP. Please consider the guidance below, and take advice from your Data Protection Officer or equivalent. Definitions of terms can be found at Appendix A.

#### **TABLES 1 & 2 – personal data and special categories of personal data**

In most cases, information sharing partners will need to:

- Select at least one lawful basis from table 1 (sharing personal data), **and**
- Select at least one lawful basis from table 2 (processing special categories of data).

Notes: Usually, only one lawful basis should be selected in table 1 and one in table 2. If more than one lawful basis is selected in either table (for example if partner organisations are relying on different lawful bases), please add an explanatory note.

#### **TABLE 3 – personal data about criminal convictions, offences etc.**

- The lawful basis for sharing personal data about criminal convictions, offences or related security measures should be recorded in table 3.
- You **will always** have to complete table 1.
- If you are sharing special categories of personal data, you will also have to complete table 2.

#### **TABLE 4 – processing by competent authorities for law enforcement purposes** (as defined by Part 3 of the Data Protection Act 2018).

- Complete table 4 only if personal data is being processed by competent authorities **and** only for law enforcement purposes.
- If information is being shared for law enforcement and other purposes you may also need to complete tables 1, 2 & 3.

**Table 1 - Article 6 - Personal Data**

Legal basis	Check box / Notes
<p>Necessary for compliance with a legal obligation – Art 6(1)(c)</p>	<p><input checked="" type="checkbox"/></p> <ul style="list-style-type: none"> <li>• <i>Social Services and Well-being (Wales) Act 2014</i></li> <li>➤ <i>Part 2 – General Functions</i></li> <li>➤ <i>Part 9 – Co-operation and Partnership</i></li> </ul> <p><b>Health Specific Legal Obligations</b></p> <ul style="list-style-type: none"> <li>• <i>National Health Service Act 1977 &amp; (Wales) Act 2006</i></li> <li>• <i>Public Records Act 1958</i></li> <li>• <i>Access to Health Records Act 1990</i></li> <li>• <i>Health &amp; Social Care Act 2012</i></li> <li>• <i>Social Services and Wellbeing (Wales) Act 2014</i></li> <li>• <i>Mental Health Act 2007 and Mental Capacity Act 2005</i></li> </ul>
<p>Task carried out in the public interest or in the exercise of official authority – Art 6(1)(e)</p>	<p><input checked="" type="checkbox"/></p> <ul style="list-style-type: none"> <li>• <i>Social Services and Well-being (Wales) Act 2014</i></li> <li>➤ <i>Part 2 – General Functions</i></li> <li>➤ <i>Part 9 – Co-operation and Partnership</i></li> </ul> <ul style="list-style-type: none"> <li>• <i>National Health Service Act 1977 &amp; (Wales) Act 2006</i></li> <li>• <i>Public Records Act 1958</i></li> <li>• <i>Access to Health Records Act 1990</i></li> <li>• <i>Health &amp; Social Care Act 2012</i></li> <li>• <i>Social Services and Wellbeing (Wales) Act 2014</i></li> <li>• <i>Mental Health Act 2007 and Mental Capacity Act 2005</i></li> </ul>

**Table 2 - Article 9 - Special Categories of Personal Data**

Legal basis	Checkbox / Notes
<p>Necessary for reasons of substantial public interest - Art 9(2)(g)</p>	<p><input checked="" type="checkbox"/></p> <p>GDPR Art 9(2)(g) requires a basis in UK law, which is provided by Section 10(3) of the Data Protection Act 2018.</p> <p>This in turn refers to the need to meet a relevant condition in Part 2 of Schedule 1 of the DPA 2018. The relevant condition is:</p> <p>Statutory and government purposes - Processing necessary for the exercise of a function conferred on a person by enactment or rule of law or the exercise of a function of the Crown, a Minister or a government department.</p> <ul style="list-style-type: none"> <li>• <i>Social Services and Well-Being (Wales) Act 2014</i> <ul style="list-style-type: none"> <li>➤ <i>Part 2 – General Functions</i></li> <li>➤ <i>Part 9 – Co-operation and Partnership</i></li> </ul> </li> <li>• <i>National Health Service Act 1977 &amp; (Wales) Act 2006</i></li> <li>• <i>Public Records Act 1958</i></li> <li>• <i>Access to Health Records Act 1990</i></li> <li>• <i>Health &amp; Social Care Act 2012</i></li> <li>• <i>Social Services and Wellbeing (Wales) Act 2014</i></li> <li>• <i>Mental Health Act 2007 and Mental Capacity Act 2005</i></li> </ul>
<p>Provision of preventative or occupational medicine, health or social care or treatment, or the management of health or social care systems – Art 9(2)(h)</p>	<p><input checked="" type="checkbox"/></p> <p>GDPR Art 9(2)(g) requires a basis in UK law, which is provided by Section 10(3) of the Data Protection Act 2018.</p> <p>This in turn refers to the need to meet a relevant condition in Part 2 of Schedule 1 of the DPA 2018. The relevant condition is:</p> <p>Health or social care - Processing necessary for health or social care purposes</p> <ul style="list-style-type: none"> <li>• <i>Social Services and Well-Being (Wales) Act 2014</i> <ul style="list-style-type: none"> <li>➤ <i>Part 2 – General Functions</i></li> <li>➤ <i>Part 9 – Co-operation and Partnership</i></li> </ul> </li> <li>• <i>National Health Service Act 1977 &amp; (Wales) Act 2006</i></li> <li>• <i>Public Records Act 1958</i></li> <li>• <i>Access to Health Records Act 1990</i></li> <li>• <i>Health &amp; Social Care Act 2012</i></li> <li>• <i>Social Services and Wellbeing (Wales) Act 2014</i></li> <li>• <i>Mental Health Act 2007 and Mental Capacity Act 2005</i></li> </ul>
<p>Public health - Art 9(2)(i)</p>	<p><input checked="" type="checkbox"/></p> <p><i>National Health Service Act 1977 &amp; (Wales) Act 2006</i></p> <ul style="list-style-type: none"> <li>• <i>Public Records Act 1958</i></li> <li>• <i>Access to Health Records Act 1990</i></li> <li>• <i>Health &amp; Social Care Act 2012</i></li> <li>• <i>Social Services and Wellbeing (Wales) Act 2014</i></li> <li>• <i>Mental Health Act 2007 and Mental Capacity Act 2005</i></li> </ul>

## 5. Personal information to be shared

- 5.1 Only the minimum necessary personal information consistent with the purposes set out in this document can be shared. Anonymised and pseudonymised information should be used where possible.
- 5.2 Information provided by partner organisations will not generally be released to any third party without prior consultation with the originating partner organisation.
- 5.3 An information reference table at Appendix B provides details of the information exchanges associated with this ISP, including the typical categories of information shared, the organisations involved and the parts of the organisation typically involved. As controllers in their own right, partner organisations are responsible for ensuring the appropriate staff have access to personal information that is adequate, relevant and limited to what is necessary for the intended purpose.
- 5.4 The following table sets out the personal information commonly shared to identify data subjects and ensure partner organisations are referring to the same data subject:

Personal identifiers	Select all that apply
Name (including aliases)	<input checked="" type="checkbox"/>
Date of birth	<input checked="" type="checkbox"/>
Address	<input checked="" type="checkbox"/>
Postcode	<input checked="" type="checkbox"/>
Other reference number (eg NHS number, National Insurance number, any system/service number )	<input checked="" type="checkbox"/>

## 6. Data Subjects' Rights

- 6.1 Data protection legislation provides various individual rights for data subjects. Advice on how these rights should be met should be sought from each organisation's Information Governance representative, Data Protection Officer or equivalent. Specific guidance on these rights is available on the Information Commissioner's website; [www.ico.org.uk](http://www.ico.org.uk)
- 6.2 The following paragraphs refer to key rights associated with sharing personal information.
- 6.3 Unless doing so would risk harm to them or others, or hinder any investigation or legal proceedings, data subjects should be informed how and why their personal information will be processed and who it is shared with (the Right to be Informed). Ideally, this information – often provided in what is commonly referred to as a privacy notice - will be provided at the first point of contact. It can be part of a registration / consent form or a standalone document.
- 6.4 A layered approach is often appropriate. This could involve a high level organisational statement supplemented by specific service level information; for example a website or leaflet and verbal information provided by a practitioner.
- 6.5 Information should be clear and particular care should be taken when relying on consent as the legal basis for sharing information, or where working with children, as there are additional requirements to consider. Further information on the 'Right to be Informed' is available on the Information Commissioner's website; [www.ico.org.uk](http://www.ico.org.uk)

6.6 For the purposes of this ISP, partner organisations should set out below how they meet the requirements of the Right to be Informed. Ideally, a consistent message will be provided and it may be helpful to agree a standard service level privacy notice.

Name of Organisation	Method of Informing (select any that apply)	Name of document / website	Comments
Intermediate Care Team (comprised of staff from the following - PCC HDUHB PAVS)	Website <input checked="" type="checkbox"/>	PCC <a href="https://www.pembrokeshire.gov.uk/privacy-promise/departmental-privacy-notice">https://www.pembrokeshire.gov.uk/privacy-promise/departmental-privacy-notice</a>	
	Leaflet <input type="checkbox"/>		
	Form <input type="checkbox"/>	Hywel Dda	
	Verbal <input checked="" type="checkbox"/>	<a href="https://hduhb.nhs.wales/about-us/governance-arrangements/your-information-your-rights/privacy-notice/">https://hduhb.nhs.wales/about-us/governance-arrangements/your-information-your-rights/privacy-notice/</a>	
	Other <input type="checkbox"/> (specify in comments)	PAVS <a href="https://www.pavs.org.uk/privacy.html">https://www.pavs.org.uk/privacy.html</a>	

6.7 All participating organisations will have in place policies and procedures to uphold the confidentiality, integrity and availability of personal information with specific reference to the retention, storage and disposal of records.

6.8 Requests for the information referenced in this ISP will be dealt with in accordance with each partner organisation's relevant policies and procedures.

6.9 Each partner organisation will put in place a formal procedure by which data subjects, partner organisations and practitioners can direct any complaints regarding the information sharing documented in this ISP.

6.10 There is an expectation that partners to this ISP will work together to keep all partners informed of any complaints or requests for information received from data subjects or third parties. The partners will also keep each other informed of any problems associated with the information sharing practices documented in this ISP and there is an expectation that they will collaborate to develop and improve these practices.

## 7. Information security

7.1 Each partner organisation must have an appropriate and adequate security framework.

7.2 Practitioners carrying out the functions outlined in this ISP should make themselves aware of, and adhere to, their organisation's information security policies and procedures.

7.3 A detailed list of agreed methods for the safe and secure transfer of personal information is documented within Appendix B.

7.4 All partners must ensure adequate and appropriate training on the subjects of data protection and confidentiality is provided to all staff with access to personal data.

---

## **8. Review of this ISP**

- 8.1 This ISP will be reviewed 6 months from signing this document, which is deliberately sooner than the WASPI guidelines as this is a rapidly emerging service and will need a more regular review as the services become more integrated. There is guidance available on the WASPI website about the process for reviewing an ISP.

## 9. Appendix A – Glossary of Terms

Term	Definition
<b>Data Protection Act 2018</b>	<p>The UK's third generation of data protection law replaces the Data Protection Act 1998. The 2018 Act accepts the standards and obligations set by GDPR and, where GDPR allows, makes specific provisions relevant to the UK.</p> <p>The 2018 Act also transposes EU Data Protection Directive 2016/680 (Law Enforcement Directive) into domestic UK law.</p> <p>It is important the GDPR and the DPA 2018 are read side by side.</p>
<b>Data Protection Officer</b>	<p>Certain categories of organisation, including any public body or authority (except courts in their judicial capacity) are required to designate a suitably qualified Data Protection Officer (DPO). The tasks of the DPO are set out in Article 39 of GDPR.</p>
<b>Data subject</b>	<p>A 'data subject' is an identified or identifiable natural person. Organisations may refer to data subjects as service users, patients, clients, citizens, etc but for consistency, WASPI framework documentation refers to data subjects.</p>
<b>GDPR</b>	<p>The General Data Protection Regulation (GDPR) lays down laws relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.</p>
<b>Law Enforcement Purposes</b>	<p>The purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. (DPA 2018 Part 3, Chapter 1, Section 31)</p>
<b>Personal data</b>	<p>'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.</p>

<b>Personal data about criminal convictions, offences or related security measures</b>	This includes personal data which relates to the alleged commission of offences by the data subject, or proceedings for an offence committed or alleged to have been committed by the data subject or the disposal of such proceedings, including sentencing. (DPA 2018 Section 11(2))
<b>Personal identifiers</b>	A set of basic personal details that allow partner organisations to identify a data subject.
<b>Personal information</b>	Includes information falling within the definition of 'personal data' and information about deceased individuals. Data protection legislation does not apply to information about deceased individuals but such information needs to be treated confidentially and WASPI should be applied to this information.
<b>Practitioner</b>	An inclusive term that refers to those involved in the care, education, welfare of data subjects; ie those who provide a public service.
<b>Processing personal data</b>	'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.' (GDPR Art 4(2))
<b>Special categories of data / sensitive processing</b>	Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. (GDPR Art 9(1))

## 10. Appendix B – Information Reference Table for the Intermediate Care Team – Pembrokeshire

This table sets out the why, what, when and how of information sharing in detail. Guidance on completing this section can be found on the website

	Description	[Referral through intermediate care hub]	[Screening]	[Intermediate care assessment, care plan and service required]	[Community services]
1	<p><b>Information exchange</b></p> <p><i>General description of the process or stage to which the information sharing relates.</i></p>	<p>Referral made through professionals (only) either from acute or community settings.</p> <p>Intermediate care hub to act as the single point of access for all intermediate care referrals, with calls taken by care-pathway co-ordinators who transcribe information onto CareFirst system.</p>	<p>If referral is deemed appropriate, then an intermediate care professional will screen, prioritise and allocate the referral.</p> <p>If referral not appropriate, care pathway co-coordinators will refer on to appropriate service</p>	<p>The initial referral will remain open for the duration of the service. Information will include details of assessment of each intermediate care professional involved in the case. Intermediate care team professional initiates a response from the following:</p> <ul style="list-style-type: none"> <li>• Acute Response Team (Hywel Dda)</li> <li>• Care at Home Team (Hywel Dda)</li> <li>• Reablement (PCC)</li> <li>• Integrated Falls Service (Hywel Dda)</li> <li>• Joint Discharge Team (PCC)</li> <li>• Community Admission Prevention / Discharge Planning (Hywel Dda)</li> <li>• Therapy teams (Hywel Dda)</li> <li>• PIVOT (PAVS)</li> </ul>	<p>Following (or during) the service as the individual is treated in the community with support from the intermediate care team, information will be shared with the PIVOT service (PAVS) to support transfer of care back home and also with the individuals local GP.</p> <p>Discharge summary forms will be shared with social services for any ongoing care and support needs.</p>

	Description	[Referral through intermediate care hub]		[Screening]		[Intermediate care assessment, care plan and service required]		[Community services]	
2	<p><b>What information will be shared?</b></p> <p><i>Describe the information to be shared – you do not need to go to ‘field level’ detail.</i></p> <p><b><u>Please note: Only the minimum and relevant personal information is to be shared and strictly on a case by case basis.</u></b></p>	<ul style="list-style-type: none"> <li>Name/address/ telephone number</li> <li>Date of Birth</li> <li>Gender</li> <li>E-number/NHS number</li> <li>GP &amp; practice</li> <li>Next of kin</li> <li>Medical and social history</li> <li>Care provider (if applicable)</li> </ul>		<ul style="list-style-type: none"> <li>Name/address/ telephone number</li> <li>Date of Birth</li> <li>Gender</li> <li>E-number/NHS number</li> <li>GP &amp; practice</li> <li>Next of kin</li> <li>Medical and social history</li> <li>Care provider (if applicable)</li> </ul>		<ul style="list-style-type: none"> <li>Name/address/ telephone number</li> <li>Date of Birth</li> <li>Gender</li> <li>E-number/NHS number</li> <li>GP &amp; practice</li> <li>Next of kin</li> <li>Medical and social history</li> <li>Details of assessment</li> </ul>		<ul style="list-style-type: none"> <li>Name/address/ telephone number</li> <li>Date of Birth</li> <li>Gender</li> <li>E-number/NHS number</li> <li>GP &amp; practice</li> <li>Next of kin</li> <li>Medical and social history</li> <li>Details of assessment</li> <li>Details of service received</li> <li>Consideration of eligibility of on-going services</li> </ul>	
3	<p><b>Partner Organisation(s)</b></p> <p><i>Details of provider and recipient organisation(s)</i></p> <p><i>Ensure the organisations listed reflect section 2 of the ISP i.e. are all organisations listed in section 2</i></p>	<p><b>Who by</b></p> <ul style="list-style-type: none"> <li>HywelDda UHB</li> <li>PCC</li> <li>WAST</li> </ul>	<p><b>Who to</b></p> <ul style="list-style-type: none"> <li>Intermediate care team (this team is the joint team made up of all partner organisations)</li> </ul>	<p><b>Who by</b></p> <ul style="list-style-type: none"> <li>HywelDda UHB</li> <li>PCC</li> <li>WAST</li> <li>PIVOT (PAVS)</li> </ul>	<p><b>Who to</b></p> <ul style="list-style-type: none"> <li>HywelDda UHB</li> <li>PCC</li> <li>PIVOT (PAVS)</li> </ul>	<p><b>Who by</b></p> <ul style="list-style-type: none"> <li>HywelDda UHB</li> <li>PCC</li> <li>WAST</li> <li>PIVOT (PAVS)</li> </ul>	<p><b>Who to</b></p> <ul style="list-style-type: none"> <li>HywelDda UHB</li> <li>PCC</li> <li>WAST</li> <li>PIVOT (PAVS)</li> </ul>	<p><b>Who by</b></p> <ul style="list-style-type: none"> <li>HywelDda UHB</li> <li>PCC</li> <li>WAST</li> <li>PIVOT (PAVS)</li> </ul>	<p><b>Who to</b></p> <ul style="list-style-type: none"> <li>HywelDda UHB</li> <li>PCC</li> <li>PIVOT (PAVS)</li> </ul>

	Description	[Referral through intermediate care hub]	[Screening]	[Intermediate care assessment, care plan and service required]	[Community services]
4	<p><b>How is information shared and what methods are used to keep the information secure?</b></p> <p><i>Provide, in detail the specific agreed secure methods for sharing personal information</i></p>	<ul style="list-style-type: none"> <li>• Telephone</li> <li>• Face to face</li> <li>• Paper copies of referral</li> <li>• Email</li> </ul> <p>In addition to the security around CareFirst any electronic personal or special category data should be sent via Transport Layer Security (TLS) email version 1.2 and higher.</p> <p>Partners will apply encryption and password protection measures in line with organisational policy.</p>	<ul style="list-style-type: none"> <li>• Paper copy</li> <li>• Telephone</li> <li>• Face to face</li> <li>• Email</li> <li>• Electronic system (CareFirst)</li> <li>• Electronic scheduling system (CM2000)</li> <li>• Fax</li> </ul> <p>In addition to the security around CareFirst any electronic personal or special category data should be sent via Transport Layer Security (TLS) email version 1.2 and higher.</p> <p>Partners will apply encryption and password protection</p>	<ul style="list-style-type: none"> <li>• Paper copy</li> <li>• Telephone</li> <li>• Face to face</li> <li>• Email</li> <li>• Electronic system (CareFirst)</li> <li>• Electronic scheduling system (CM2000)</li> <li>• Fax</li> </ul> <p>In addition to the security around CareFirst any electronic personal or special category data should be sent via Transport Layer Security (TLS) email version 1.2 and higher.</p> <p>Partners will apply encryption and password protection</p>	<ul style="list-style-type: none"> <li>• Paper copy</li> <li>• Telephone</li> <li>• Face to face</li> <li>• Email</li> <li>• Electronic system (CareFirst)</li> <li>• Electronic scheduling system (CM2000)</li> <li>• Fax</li> </ul> <p>In addition to the security around CareFirst any electronic personal or special category data should be sent via Transport Layer Security (TLS) email version 1.2 and higher.</p> <p>Partners will apply encryption and password protection</p>
5	<p><b>Reliance on consent</b></p> <p><i>Check the box if any exchange relies on consent and explain how and when consent is obtained. Ensure section 4 of the ISP reflects this legal basis</i></p>	<p><input type="checkbox"/> Exchange relies on consent</p> <p><input checked="" type="checkbox"/> Exchange does not rely on consent</p>	<p><input type="checkbox"/> Exchange relies on consent</p> <p><input checked="" type="checkbox"/> Exchange does not rely on consent</p>	<p><input type="checkbox"/> Exchange relies on consent</p> <p><input checked="" type="checkbox"/> Exchange does not rely on consent</p>	<p><input type="checkbox"/> Exchange relies on consent</p> <p><input checked="" type="checkbox"/> Exchange does not rely on consent</p>
6	<p><b>Notes for Practitioners</b></p>				

---

## **11. Appendix C – Partner Organisations Signatures**

This section should only be completed once the ISP has been assured by a Quality Assurance group. Further information on the ISP development process can be found on the WASPI Website.

By signing below, partner organisations are confirming they agree with the content of the ISP. In the context of sharing personal information, signing the ISP is one way to demonstrate accountability with the principles set out in Article 5 of GDPR.

The signatory will be an appropriate person with authority to sign the ISP on behalf of the organisation. The ISP lead has responsibility for obtaining signatures to the ISP.

## **12. Appendix D – WAST Data Disclosure Agreement**



DDA Intermediate  
Care Team draft.doc