





## Wales Accord on the Sharing of Personal Information

# Information Sharing Protocol for CRT Together - Cwm Taf Morgannwg University Health Board Region

Version V1.0

Date Assured 10.05.2024

Quality Assurance Group Cwm Taf

## Contents

1	Introduction to this ISP	1
2	The information sharing partner organisations	2
3	Specific organisational / practitioner obligations	3
4	Legislative / statutory powers	3
5	Personal information to be shared	5
6	Data Subjects' Rights	5
7	Information security	7
8	Review, Breaches and Termination of this Agreement	7
9	Appendix A – Glossary of Terms	9
10	Appendix B – Information Reference Table	11

### **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 CRT Together programme across the Cwm Taf Morgannwg University Health Board region.
- 1.4 Personal information is shared for the purpose of delivering a conditions specific non-clinical service to improve the cancer journey of individuals/patients. The CRT Together programme will help people diagnosed with cancer to complete an electronic holistic needs assessment and may also support carers and family members. This ISP will enable referrals from the Cwm Taf Morgannwg University Health Board to CRT Together and the sharing of information to improve the level of support provided to individuals.

## 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
The Coalfields Regeneration Trust (CRT)	Development Manager – CRT Together	CRT Together
The Coalfields Regeneration Trust (CRT)	Quality Assurance Co-ordinator (data protection lead) (Point of contact)	Corporate Services
Cwm Taf Morgannwg University Health Board	Executive director Digital (Owner)	Planned care, Unscheduled care, Primary care, women and child health, Pathology (service groups)  All services supporting cancer patients including surgical team, Medical teams, primary care teams and Haematology
Cwm Taf Morgannwg University Health Board	Macmillan lead nurse for cancer services (Point of contact)	Cancer services

- 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.

---

### 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 UK 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
Consent – Art 6(1)(a)	<input checked="" type="checkbox"/> <i>Consent will be obtained for the Health Board to send a CRT Together Registration Form to CRT on behalf of the patient and for CRT to share support updates with the Health Board.</i>

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

Legal basis	Checkbox / Notes
Explicit Consent – Art 9(2)(a)	<input checked="" type="checkbox"/> <i>Consent will be obtained for the Health Board to send a CRT Together Registration Form to CRT on behalf of the patient and for CRT to share support updates with the Health Board.</i>

## 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 type="checkbox"/>
	<input 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](http://www.ico.org)
- 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
Coalfields Regeneration Trust	Website <input checked="" type="checkbox"/> Leaflet <input type="checkbox"/> Form <input checked="" type="checkbox"/> Verbal <input checked="" type="checkbox"/> Other (specify in comments) <input type="checkbox"/>	CRT Together Privacy Policy, Registration Form and Participant Agreement.	<p>This document is available to individuals on the Coalfields Regeneration Trust <a href="#">Website</a></p> <p>Appendix A.</p> <p> Appendix A CRT Together Privacy Polic</p> <p>The Form contains a privacy statement.</p> <p>The Form including how information provided will be used will be discussed with the patient during referral. This is reiterated by the CRT Together staff during the initial contact when arranging the first appointment.</p> <p>Form Appendix B.</p> <p> Appendix B CRT Together Registration</p> <p>The CRT Together Agreement includes a section on data protection, confidentiality and how information will be used. Throughout the service CRT Together staff will discuss sharing personal data with the individual prior to sharing it with Health Board to ensure the individual remains informed.</p> <p>This agreement is discussed with the individual prior to them signing it to ensure they: understand; are</p>

			<p>happy with the content; and have no queries.</p> <p>Agreement Appendix C.</p>  <p>Appendix C CRT Together Participant /</p>
Cwm Taf Morgannwg University Health Board	<p>Website <input checked="" type="checkbox"/></p> <p>Leaflet <input type="checkbox"/></p> <p>Form <input type="checkbox"/></p> <p>Verbal <input type="checkbox"/></p> <p>Other (<i>specify in comments</i>) <input type="checkbox"/></p>	Privacy Statement	<p>The health board's privacy statement is available online here <a href="https://ctmuhb.nhs.wales/use-of-site/privacy-policy/">https://ctmuhb.nhs.wales/use-of-site/privacy-policy/</a></p> <p>Plus, health board staff will complete the above Registration Form (Appendix B) with the patient.</p>

- 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, Breaches and Termination of this Agreement

- 8.1 This ISP will be reviewed two years from signing this document or sooner if appropriate. There is guidance available on the WASPI website about the process for reviewing an ISP.

- 
- 8.2 Breaches of this agreement should be reported to the Owners / Contact Points in Section 2, which may result in the information sharing set out in this agreement ceasing.
  - 8.3 Partners to this agreement will determine the responsibilities following termination of this agreement, including the deletion of shared data or its return to the organisation that supplied it originally.

## 9 Appendix A – Glossary of Terms

Term	Definition
<b>Appropriate Policy Document</b>	<p>The Data Protection Act 2018 outlines the requirement for an Appropriate Policy Document to be in place when processing special category and criminal offence data under certain specified conditions.</p> <p>Detail on Appropriate Policy Documents can be found in Schedule 1, Part 4 of the DPA 18 and Section 42 of the DPA 18 for competent authorities.</p>
<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 UK GDPR and, where UK 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 UK 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 UK 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>UK GDPR</b>	<p>The UK General Data Protection Regulation (UK 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.' (UK 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. (UK GDPR Art 9(1))
<b>e-HNA</b>	Electronic Holistic Needs Assessment. The assessment can be carried out at any stage of the cancer pathway, to help you: <ul style="list-style-type: none"> <li>• identify a patient's concerns</li> <li>• start a conversation about needs</li> <li>• develop a Personalised Care and Support Plan (care plan)</li> <li>• share the right information, at the right times</li> <li>• signpost to relevant services.</li> </ul>

## 10 Appendix B – Information Reference Table for CRT Together - Cwm Taf Morgannwg University Health Board Region

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	HNA Care Plan	[Insert title of exchange 3]	[Insert title of exchange 4]
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>When a patient wishes to receive support from the CRT Together programme a CRT Together Registration Form will be completed with the patient's details and securely sent to <a href="mailto:together@coalfields-regen.org.uk">together@coalfields-regen.org.uk</a> to refer them onto the programme.</p>	<p>CRT Together team will support individuals completing their holistic needs assessment to create a personalised care plan. This will be used to provide support and identify signposting. Relevant sections of completed care plans will be shared with the Health Board to ensure awareness.</p>	<p>[Insert brief description of sharing at this point]</p>	<p>[Insert brief description of sharing at this point]</p> <p>[Where ISP has more than 4 exchanges, you may wish to use the Excel version of Appendix B available on the WASPI website]</p>

	Description	Referral		HNA Care Plan		[Insert title of exchange 3]		[Insert title of exchange 4]	
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>	Personal identifiers Demographic data Health / wellbeing information Risks/issues		Personal identifiers  Health / wellbeing information					
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> <p>Cwm Taf Morgannwg University Health Board</p>	<p><b>Who to</b></p> <p>The Coalfields Regeneration Trust (CRT) – CRT Together team</p>	<p><b>Who by</b></p> <p>The Coalfields Regeneration Trust (CRT) – CRT Together team</p>	<p><b>Who to</b></p> <p>Cwm Taf Morgannwg University Health Board</p>	<p><b>Who by</b></p>	<p><b>Who to</b></p>	<p><b>Who by</b></p>	<p><b>Who to</b></p>

	Description	Referral	HNA Care Plan	[Insert title of exchange 3]	[Insert title of exchange 4]
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>	<p>Secure File Sharing Portal</p> <p>The portal generates a password protected (encrypted) email and then sends a password to open the encrypted email separately.</p>	<p><b>Egress Protect</b></p> <p>This is secure email encryption software. The encryption is end to end.</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 checked="" type="checkbox"/> Exchange relies on consent</p> <p><input type="checkbox"/> Exchange does not rely on consent</p> <p>Consent to share is obtained in the CRT Together Registration Form.</p>	<p><input checked="" type="checkbox"/> Exchange relies on consent</p> <p><input type="checkbox"/> Exchange does not rely on consent</p> <p>Consent to share is obtained in the CRT Together Registration Form. It is also discussed at when completing the care plan and recorded on the care plan.</p>	<p><input type="checkbox"/> Exchange relies on consent</p> <p><input type="checkbox"/> Exchange does not rely on consent</p> <p><b>[If relying on consent to share, how and when is it obtained and how it is documented?]</b></p>	<p><input type="checkbox"/> Exchange relies on consent</p> <p><input type="checkbox"/> Exchange does not rely on consent</p> <p><b>[If relying on consent to share, how and when is it obtained and how it is documented?]</b></p>
6	<p><b>Notes for Practitioners</b></p>	<p>Any issues/concerns (risks) that CRT Together may need to be aware of will be sent via secure email (encrypted).</p> <p>When the CRT Together team receives a referral the Team Support Officer will assign a Link Worker (full team will have access to the referral inbox).</p>	<p>Email sent to the Health Board will include a statement that the patient has attended the appointment and they have been referred to relevant services.</p>		