Cefnogir gan
Lywodraeth Cymru
Supported by
Welsh Government

Wales Accord on the Sharing of Personal Information

Joint Controller Agreement

Joint Controller Agreement for Clinical In-Reach to Cluster Practices between the parties set out in Appendix D

Template developed in partnership with

BLAKE MORGAN

Further information on how a Joint Controller Agreement should be developed is contained within the

Guide on the Development of a Joint Controller Agreement

Further guidance may be sought from the

WASPI Service Integration and Development Team at:
www.waspi.org

Note: This page can be removed once the JCA development has commenced

Template developed in partnership with

BLAKE MORGAN

1.1	A Joint Controller Agreement (JCA) is intended to help practitioners understand what decisions have been made about the processing of Personal Data between a number of partners.
1.2	A JCA provides assurance that the partners have considered the requirements of data protection legislation as joint controllers and that each have identified their roles and responsibilities.
1.3	Organisations who use the WASPI JCA template need to ensure that any completed JCA is legally binding from their own organisational requirements. The WASPI service will not provide any opinions on any proposed agreements, data protection advice should be sought from relevant organisation's Data Protection leads.
1.4	The template JCA was developed by WASPI in partnership with Blake Morgan LLP. This template JCA has been prepared solely for the benefit of WASPI only. Whilst other organisations may use this JCA template, neither WASPI nor Blake Morgan shall owe any duty of care to any other entities and all liability of WASPI and Blake Morgan LLP to all other entities is hereby excluded. Other entities are advised seek their own advice on the contents and use of this template.

Template developed in partnership with

BLAKE MORGAN

Contents

1 Front Sheet

A.	**Parties**	See Signatories in Appendix B
B.	**Agreement Administrators**	CAVUHB – Information Governance Manager
C.	**Purpose**	The overall purpose of the activity is effective delivery of direct care for patients, including the necessary recording of interactions with patients. Clinics provided within a secondary care setting can also be delivered within GP practices. In doing so, patients benefit from reduced travel and easier access to their usual GP practice than to health board premises. Clinic delivery on GP premises also allows for GPs to encounter clinic providers and expand their knowledge and experience of clinic-related activity. The details provided in this document explain how clinicians will update GPs about their interactions with patients.
D.	**Authorised Users**	Clinicians attending clinics being held within GP / cluster practices; GPs who refer patients to those clinics, and other members of the practice team.
E.	**Commencement Date**	2nd day of January 2025
F.	**Duration of the Processing**	The contract will commence on 2 January 2025 and will continue until 31 March 2027
G.	**Categories of Personal Data**	Patient data relating to aspects of their health considered within the in-reach clinics. The data processed will therefore relate to aspects of physical and mental health and may include

		data relating to test / examination results. In order to ensure safe and continuity of care, identifying information will also be processed, including name, address, date of birth and NHS number.
H.	**Legal Bases for Processing**	See Appendix B
I.	**Agreed Sharing Mechanisms**	During interaction with the patient while attending the clinic at GP / Cluster practice, clinicians will record the subject of discussion, any investigations / assessments carried out and the results of the interaction, including diagnosis and recommendation for treatment. This information is recorded in a web app designed and managed by CAVUHB. While at the practice, the clinic providers will be able to access data held within GP systems (via application provided by Black Pear) in order to facilitate their interactions with the patient. This data will also be presented in the web app. The web app will then rely upon the Black Pear product to interact with the GP systems to transfer the data recorded in the web app through to the GP record. The health board will draw down data relating to clinics delivered by its staff using a secure download facility provided by Black Pear.
J.	**Security**	Clinic staff will only have access to the GP record of patients while they are present in the practice, accessing necessary information only. Clinic staff will be using secure practice equipment only. Initially strong passwords will be used to access the Black Pear product. Users are authenticated using Black Pear's secure BP Auth

		service using a unique user identity (their email address) in conjunction with a password. Credentials cannot be used for authentication until the user has verified their identity (i.e. email address) and set a strong password. Password strength is checked using Dropbox's zxcvbn library and only passwords that are estimated to take more than 1010 attempts to guess are allowed. Passwords are salted and hashed using an NHS approved algorithm before being stored in a secure database managed by Black Pear. Passwords will expire after 90 days and a new password must be chosen; this cannot be one of the previous 12 passwords used. The login system enforces a timeout mechanism to prevent brute-force attacks and enhance security. The timeout duration increases based on the number of consecutive failed login attempts. After 3 failed attempts the lockout imposes a delay of 5s on every attempt. After 10 attempts, the delay increases to 20s per attempt. connections between the web app and the Black Pear solution will be secured by strong passwords (see Appendix E). MFA will be incorporated during the course of the contract with Black Pear. . With full implementation, the Black Pear will be accessed using MFA via the Web App developed by CAVUHB. (This position is recognised as a risk within the DPIA produced to support this work.) Once implemented, connection to the Black Pear system by the web app is protected by security tokens relating to the clinician and the patient so that each session can

		only relate to a single patient at a time. Cluster / practice administration will administer the systems access of clinicians on site. This will be the only route to the web app interface, and therefore to the Black Pear back-end. Connection from Black Pear to write to the GP systems will be carried out using an existing or modified secure API and data in transit will be encrypted end-to-end using TLS and AES-256. A cyber assessment has been carried out.
K.	**Confidentiality Compliance**	Patients will be aware that their GP is referring them to a clinic. Data processing will be for direct care purposes. Data processing will therefore satisfy the common law duty of confidentiality. Clinicians attending at practices will be reminded of their confidentiality obligations to the GP data they may access while at the practice. (See paragraph 22.13 for details.)
L.	**Review data / frequency**	This agreement will be reviewed in one year initially and every two years subsequently.
M.	**Governance**	See Appendix C.

2 Introduction

2.1 This Joint Controller Agreement (**JCA**) is supplementary to the Wales Accord on the Sharing of Personal Information (**WASPI**) and has been agreed following consultation between the participating partner organisations.

2.2 This JCA is intended to help practitioners understand what decisions have been made about the processing of Shared Personal Data between the listed partners for the stated purpose(s).

2.3 It also provides assurance that the partners have considered the requirements of data protection legislation as joint controllers and that each have **identified their roles and responsibilities** for processing Shared Personal Data jointly. The JCA sets out these requirements under Article 26 of the UK General Data Protection Regulation (UK GDPR).

2.4 It is intended that this agreement is to be read alongside the Data Protection Impact Assessment (DPIA) prepared by the parties.

2.5 It sets out the framework for the for the sharing and processing of Shared Personal Data for the Purpose.). The JCA defines the principles and procedures that the Data Controller Parties will adhere to and the responsibilities of each party as joint controllers in relation to the sharing and use of Shared Personal Data in the delivery of the Purpose.

2.6 All Partners have entered this JCA to demonstrate that data protection and privacy requirements have been considered, to set out how use of information meets the data protection principles, and how rights of data subjects are protected. All Partners agree to observe all the obligations set out in this JCA and to comply with the data protection legislation.

2.7 This JCA does not replace any contractual arrangement as between the Parties or any requirements for data processing agreements or data sharing agreements with any third party suppliers of any goods and/or services to deliver the Purpose.

2.8 This JCA has been prepared solely for the benefit of WASPI only. WASPI nor Blake Morgan shall owe no duty of care to any other entities and such other entities are advised seek their own advice on the contents and use of this template.

3 Purpose

Personal data is processed by and shared between the Parties for the purpose of set out in the Front Sheet only.

4 The Joint Controller Partner Organisations and Responsibilities

4.1 The table below sets out the organisational partners to the JCA and the partners roles and responsibilities in relation to the joint controllership arrangement for the purposes described in this JCA.

	(A) Controller Organisations	(B) Owner / Point of contact	(C) Departments / Divisions / Teams	(D) Organisation's Role and Responsibilities / Activities

Party A	Cardiff and Value University Health Board	Information Governance Manager	Information Governance	Delivering clinics within GP / Cluster practices. Provides cluster administration and management staff Provisioning of web app and Black Pear system to facilitate data exchange.
Party B	[GP Practices]	[Insert JCA owner / point of contact – Specify roles not individual names]	[Insert departments / divisions]	Hosting clinics. Providing access to equipment during clinic.
Party C	[Insert further rows as necessary]			

4.2 Where the parties to this JCA may be public authorities, they are designed as public authorities for the purposes of the UK GDPR.

4.3 The JCA owners / points of contact have overall responsibility for this agreement within their respective organisations and must therefore ensure the JCA is disseminated, understood and acted upon by relevant practitioners.

4.4 The owners / point of contact for each partner organisation will regularly monitor and review the use of this JCA to ensure information is shared effectively and appropriately.

4.5 Each partner organisation will nominate a signatory to sign the JCA at Appendix D. The signatory will be an appropriate person from the partner organisation who can sign on behalf of the organisation.

5 Commencement and Duration

5.1 This JCA shall commence on the Commencement Date and shall continue in force until brought to an end in accordance with clause 11 or until the termination or expiry of the Purpose.

6 Specific Organisational / Partner Obligations

6.1 Practitioners who share information in line with this JCA 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.

6.2 Each Party will not disclose or allow access to the Shared Personal Data to anyone other than the Parties without the prior written authorisation of the Data Discloser and always subject to compliance with relevant safeguards and Data Protection Legislation.

6.3 Every reasonable step should be taken to ensure that inaccurate Shared 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).

7 Data breaches, complaints and investigations

7.1 Each Party will notify the other Parties who are or foreseeably may be affected or implicated as soon as reasonably possible if it becomes aware of any breach of this JCA, any breach of any of the Data Protection Legislation regarding the Shared Personal Data, any Personal Data Breach affecting any Shared Personal Data. Any Party that gives such notification shall provide the other Parties as soon as reasonably possible with such information regarding such breach as may be reasonably requested by any of the other Parties.

7.2 Any breaches of security, confidentiality and other violations of this JCA must be reported in line with each partner organisation's incident reporting procedures. Specifically, this includes the reporting, management and notification of personal data breaches between the partner organisations and should operate a shared procedure for such. Consideration should be given to sharing the outcome of any investigation, where appropriate, with other partners to the JCA.

7.3 The DPO of the Party responsible for the breach will assess and consider whether the personal data breach requires to be reported to the ICO. A log of personal data breaches will be maintained by the DPO of the responsible Party.

7.4 Each Party (the **"Originating Party"**) will give written notice to the other Parties who are or foreseeably may be affected or implicated (the **"Relevant Parties"**), as soon as reasonably possible, if the Originating Party or any of its Processors or Permitted Third Party Controllers receive(s) any request, complaint, notice, order or communication which relates directly or indirectly to the processing of any Shared Personal Data or to compliance with the Data Protection Legislation and, at the same time, will forward a copy of that request, complaint, notice, order or communication to all Relevant Parties. The Originating Party and each of the Relevant Parties will co-operate with each other and give each other such information and assistance as any other such Party may reasonably require in relation to that request, complaint, notice or communication to enable the other such Parties to respond to the same in accordance with any deadline and any requirement to provide information.

8 Legislative / Statutory Powers

8.1 The arrangements described in this JCA considers the relevant **data protection legislation**, the **Human Rights Act 1998** and the **Common Law Duty of Confidentiality (if applicable)**.

Lawful basis

8.2 Before sharing or processing Shared Personal Data, partner organisations must have identified a clear legal basis for doing so. The bases for lawful processing will depend on the individual purposes and will be assessed on a case-by-case basis. The bases for lawful processing under the UK GDPR Article 6 and conditions for processing under special category data under Article 9 will be identified and approved in DPIAs conducted prior to implementing activities that involve joint processing and information sharing. The lawful basis/es will be set out in Appendix B.

8.3 The Parties will publish their bases for lawful processing and conditions for processing special category data within their privacy notices.

8.4 Partner organisations also need to ensure they consider 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.

Common Law Duty of Confidentiality

8.5 Relying on consent to process Shared Personal Data (under Article 6(1)(a) of the UK GDPR) as a lawful basis to process personal data should not be confused with consent under Common Law Duty of Confidentiality. The two are separate and should not be confused or merged.

8.6 The Parties agree that when introducing measures to enable joint working, that they must satisfy the requirements of the Common Law Duty of Confidentiality to data subjects.

8.7 The common law duty of confidentiality is the general position that if information is given in circumstances where it is expected that a duty of confidence applies, that information cannot normally be disclosed without the information provider's agreement. Generally, the common law allows disclosure of confidential information only if the individual consents to its disclosure, it is required by law (e.g. by statute or by court order) or it is justified in the public interest.

8.8 The Parties will achieve this by addressing confidentiality requirements in the application of data protection by design and default and identifying the legal gateways to demonstrate how processing has considered and satisfied a duty of confidence.

9 Data Protection Principles, Accountability and Demonstrating Data Protection Compliance

9.1 The parties have entered into this JCA to assist them with processing Shared Personal Data in accordance with the data processing principles set out in Article 5 of the UK GDPR which are, in summary that Shared Personal Data shall be:

9.1.1 processed lawfully, fairly and in a transparent manner;

9.1.2 collected for specified, explicit and legitimate purposes;

9.1.3 adequate, relevant and limited to what is necessary;

9.1.4 accurate and, where necessary, kept up to date;

9.1.5 kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; and

9.1.6 processed in a manner that ensures appropriate security of the personal data.

9.2 Additionally, accountability is another key principles in data protection law and Parties are responsible for complying with the legislation and must be able to demonstrate their compliance. Each Party is responsible either solely or jointly for the following:

9.2.1 A single Data Protection Officer (DPO) is appointed for their central functions as controllers.

9.2.2 Each Party shall ensure that its Polices, Privacy Notice(s) and Data Protection Impact Assessments take full account of shared personal data and the processing under this JCA and made available to each Party upon its request.

9.2.3 The Parties will collaborate to ensure that a data protection by design and default approach is applied when implementing a new project, process, system or new joint working practices. This includes ensuring a DPIA has been

completed for uses of personal and pseudonymised data and obtaining approval for completed DPIAs through established governance processes.

9.3 The Parties will establish:

9.3.1 A DPIA to identify the purpose and nature of processing activities as joint or sole controllers, and the legal bases for processing and sharing Shared Personal Data, where the processing is likely to result in a high risk to the rights and freedoms of individuals, or where parties agree that a DPIA is required (or an assessment of high risk processing).

9.3.2 Information Sharing Agreements where these are applicable to the joint controller arrangement.

9.3.3 Written contracts with organisations, or a Party that processes personal data on behalf of a controller.

9.4 UK GDPR Article 30 requires organisations to maintain documentation of processing activities, referred to as Records of Processing Activities (**ROPA**). Each Party will record their processing activities to include joint controller responsibilities where these apply, and the specific information required under this Article.

9.5 The Parties will ensure they have implemented appropriate security measures for the sharing and handling of Shared Personal Data. This is demonstrated through the completion of a due diligence process that will provide assurance that a secure system/process is in place.

10 Data Subjects' Rights and Privacy Information

10.1 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

10.2 The following paragraphs refer to key rights associated with processing and sharing personal information.

10.3 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). The Parties will collaborate to ensure appropriate privacy information is provided to data subjects in a concise, transparent, and easily accessible form. Generally, online privacy notices are provided as the method of informing data subjects about the processing and sharing of their personal and special category data.

10.4 Each Party shall comply with the exercise by Data Subjects of their rights under Data Protection Legislation in accordance with this JCA.

10.5 The Party in receipt of the request to exercise the data subject rights shall primarily be responsible for responding to such requests.

10.6 The Parties each agree to assist as is reasonably required to enable the other Parties to comply with requests from Data Subjects to exercise their rights under the Data Protection Legislation within the time limits imposed by the Data Protection Legislation. Each Party will, on the request of any other Party:

10.6.1 promptly inform the other Parties about the receipt of any data subject access request and any other data subject rights request under the Data Protection Legislation.

10.6.2 provide the other Parties with reasonable assistance in complying with any data subject access request.

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

11 Information security

11.1 Each Party will take (and procure that its processors and other controllers it may share personal data with will take) appropriate technical and organisational measures (as defined in the Data Protection Legislation) to prevent unauthorised or unlawful processing of the personal data or the accidental loss or destruction of, or damage to, the personal data. Such technical and organisational measures shall ensure a level of security appropriate to the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage and the nature of the personal data to be protected.

11.2 Each Party shall implement any security measures specified in the Front Sheet and such other security measures as are at any time approved and agreed by the parties. The Parties shall keep such security measures under review and shall carry out such updates as they agree are appropriate throughout the duration of this JCA.

11.3 Each Party must have an appropriate and adequate security framework.

11.4 The Parties 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.

11.5 Each Party shall ensure, within its own organisation, that there is no disclosure of Personal Data to any person (including the Party's own Staff who are not Authorised Users, and including other Parties as well as third parties) where such disclosure would be in breach of any duty of confidence. Each Party shall ensure that the Processing of the Shared Personal Data is only performed by that Party's Authorised Users and that such Authorised Users have received appropriate training.

11.6 Each Party carrying out the specific roles and responsibilities outlined in this JCA should be aware of, and adhere to, their organisation's information security policies and procedures.

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

11.8 Each Party shall only disclose the Shared Personal Data to other Parties solely via the Agreed Sharing Mechanisms set out in the Front Sheet.

12 Data Retention and Deletion

12.1 The Parties shall not retain or process Shared Personal Data for longer than is necessary to carry out the Purpose.

12.2 Notwithstanding clause 8.1, Parties shall continue to retain Shared Personal Data in accordance with any statutory or professional retention periods applicable.

13 International transfers of personal data

13.1 The Parties will not as standard transfer the Shared Personal Data outside of the UK or European Economic Area for the purposes of the delivery of the Purpose.

14 Governance and decision making

14.1 The Parties shall set out the governance and decisions-making process in respect of this JCA in Appendix C.

15 Variation

15.1 All Parties may request a change to the existing JCA through written notification to the other Parties.

15.2 All proposed changes will be discussed between the Data Protection Officers (DPOs) of all Parties of this JCA. Any changes that are agreed and implemented between the Parties will be incorporated into this JCA at the next revision of this JCA (with any amendment of variation only coming into effect once the amended or varied JCA is signed by all Parties) and also reflected in respective DPIA and Privacy Notice.

15.3 External changes affecting the operational delivery responsibilities of the Parties will also necessitate the review and potential amendment of the JCA.

15.4 All Parties to this JCA are expected to make every effort to ensure that any changes to the JCA are implemented with minimal disruption.

16 Termination

16.1 This JCA shall automatically terminate upon the expiry or termination of the Purpose.

16.2 Any Party may terminate its participation in this JCA at any time by serving no less than twenty (20) working day's written notice to the duly designated Agreement Administrator.

16.3 A Party shall immediately cease to be a Party to this JCA if they cease to be a member of the Purpose.

16.4 In the event that a Party's membership of the JCA is terminated, an amended and updated version of this JCA will be drafted as soon as practicable and circulated to all other Parties by the duly designated Agreement Administrator.

16.5 Each Party shall, on the termination of its membership of this JCA:

16.5.1 cease to store, access and otherwise Process the Shared Personal Data that was made available to it by any Data Discloser under or in connection with this JCA (and shall procure that its Processors shall cease to so disclose Shared Personal Data); and

16.5.2 cease to disclose Shared Personal Data under or in connection with this JCA (and shall procure that its Processors shall cease to so disclose Shared Personal Data).

16.5.3 remove reference to the JCA and the Shared Personal Data in any Privacy Notice under its control; and

16.5.4 remove the interfaces and other means by which the relevant Party's Electronic Information Processing Systems are connected with the remaining Parties' Electronic Information Processing Systems (and each of them).

16.6 Data Subject rights or any statutory duties or obligations incurred under Data Protection Legislation by any Party to this JCA and which survive the expiry or termination of this Agreement will continue after expiry or termination.

17 Liability

17.1 Nothing in this Agreement is intended to limit any Party's liability in respect of the exercise of any of its statutory functions or its obligations to comply with Data Protection Law.

18 Dispute Resolution

18.1 If either party has any issues, concerns or complaints about the JCA, or any matter in this JCA, that Party shall notify the other Party and the parties shall, acting in good faith, seek to resolve the issue by negotiations between themselves. If the issue cannot be resolved within 7 days, the matter shall be escalated to the nominated representative and the Data Protection Officer who shall advise on the appropriate course of action to take.

18.2 Any disagreement between the Parties regarding the application of this JCA will normally be resolved at working level. If this is not possible, it may be referred through those responsible for the management of this JCA, up to and including the heads of the organisations (e.g., Chief Executive / Permanent Secretary) who will then jointly be responsible for ensuring a mutually satisfactory resolution.

18.3 If the dispute cannot be resolved by the above contacts in clause 13.1 within 14 days, they shall seek legal advice.

19 General

19.1 The JCA is not intended to be legally binding, and no legal obligations or legal rights will arise between the Partners from this JCA. The Partners enter the JCA intending to honour all their obligations, including compliance with Article 26 UK GDPR and Section 58 Data Protection Act 2018 (DPA 2018), regarding requirements for joint controllers.

19.2 Nothing in this JCA is intended to, or will be deemed to, establish any agreement or joint venture between the Partners, constitute any Partner as the agent of the other Partner, nor authorise the Partners to make or enter any commitments for or on behalf of the other Partner.

19.3 The JCA will be governed by and construed in accordance with English and Welsh law (as it applies in Wales).

20 Appendix A – Glossary of Terms

Term	Definition
Agreed Sharing Mechanism	Means the technical measures described in the Front Sheet, being the means by which the Parties shall transmit Shared Personal Data between each other.
Agreement Administrator	The individual appointed by the Joint Controllers to be responsible for administering this JCA for and on behalf of the Parties.
Authorised User	Means, in relation to each Party, each member of its Staff who: a) falls within any one of the categories specified in (as applicable) the Privacy Notices; and b) is authorised by that Party to Process the relevant Shared Personal Data for the purposes stated in such Privacy Notices;
Controller	Has the meaning given to it in the UK GDPR. Controllers are the main decision-makers, they exercise overall control over the purposes and means of the processing of personal data.
Data Discloser	Means a Party who makes available any Shared Personal Data to another Party.
Data Protection Impact Assessment	Means, for each Party, its completed data protection impact assessment as prepared by it in accordance with the Data Protection Legislation.
Data Protection Act 2018	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. The 2018 Act also transposes EU Data Protection Directive 2016/680 (Law Enforcement Directive) into domestic UK law. It is important the UK GDPR and the DPA 2018 are read side by side.
Data Protection Officer	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.
Data subject	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.

Direct Care	1. A clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals. It includes supporting individuals' ability to function and improve their participation in life and society. It includes the assurance of safe and high quality care and treatment through local audit, the management of untoward or adverse incidents, person satisfaction including measurement of outcomes undertaken by one or more registered and regulated health or social care professionals and their team with whom the individual has a legitimate relationship for their care. 2. Direct care is provided by health and social care staff working in care teams, which may include doctors, nurses and a wide range of staff on regulated professional registers, including social workers. Relevant information should be shared with them when they have a legitimate relationship with the patient or service user.
UK GDPR	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.
Joint Controller	If two or more controllers jointly determine the purposes and means of processing the same personal data.
Law Enforcement Purposes	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).
Personal data	'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.
Personal data breach	Has the meaning given to it in the UK GDPR and includes also any breach of Article 5(1)(f) (the integrity and confidentiality principle) of the UK GDPR.
Personal data about criminal convictions, offences or related security measures	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))

Personal information	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.
Practitioner	An inclusive term that refers to those involved in the care, education, welfare of data subjects; ie those who provide a public service.
Processing personal data	'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))
Purpose	An inclusive term that refers to the purpose/project/service/programme for which this Joint Controller Agreement relates to (as set out in the Front Sheet).
Pseudonymised data	Means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable individual.
Special categories of data / sensitive processing	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))

21 Appendix B – Lawful basis/es

Table 1 - Article 6 - Personal Data

Legal basis	21.1 Check box / Notes
Task carried out in the public interest or in the exercise of official authority – Art 6(1)(e)	☒ *21.2 Primary care services are delivered in line with the requirement to provide health services across Wales as set out in NHS (Wales) Act 2006 and related legislation and guidance.* *21.3 The processing described in this DPIA is being carried out in order to carry out the public tasks of the local health board and the Clusters of GP practices within the HB footprint.*

	21.4 In order to permit the Local Health Board to support work provided within primary care, National Health Service (Wales) Act 2006 (legislation.gov.uk) – Section 53 permits a Local Health Board to 'provide assistance or support to any person providing or proposing to provide … primary medical services under a general medical services contract'. *21.5 Local Health Board may provide assistance or support on terms the Local Health Board considers appropriate.* *21.6 Section 53 is further enabled by The Local Health Boards (Directed Functions) (Wales) Regulations 2009 (legislation.gov.uk), the Schedule of which identifies actions exercisable under S53 of NHS(W)A 2006: "Providing assistance and support in relation to primary medical services".* *21.7 In the present case, the LHB has deemed it appropriate to support the provision of technical and administrative support to facilitate community delivery of secondary health care clinics within Cluster practices.* *21.8 While there is no specific legislation relating to the work of GP clusters, there is a clear direction of travel toward this model, as evidenced by the ministerial letter and funding provided for Accelerated Cluster development. Further information is accessible on the Primary Care One website.* *21.9 Expectations on cooperation between GP practices within Clusters are also covered by regulations relating to health board finances (LHBs fund Clusters) and within the General Medical Services (GMS) contract.*

Table 2 - Article 9 - Special Categories of Personal Data

Legal basis	21.10 **Checkbox / Notes**
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)	☒ *21.11 The processing of data under this agreement is carried out by or under the responsibility of health professionals: staff will be delivering clinics to patients referred by their GP, and providing feedback to the latter.* *21.12 Legislative provisions are as set out in Table 1 relating to Article 6, principally the NHS (Wales) Act 2006.]*

22 Appendix C – Governance and decision making

22.1 [Contractual Obligations

22.2 Appropriate contracts will be drawn up to define responsibilities of the partners, particularly with regard to the data processor (Black Pear). The contracts will cover aspects of resilience, data security, data retention and other privacy compliance topics.

22.3 Controller / Processor

22.4 With respect to the component parts of the process, the following controller and processor arrangements are in place.

22.5 The web app which clinic staff will use to record their interactions with patients will be provided and managed by CAVUHB. However, its' design and decisions about its use have been, and will continue to be, jointly developed between the parties – that is, the Local Health Board and participating GP Clusters / practices. This Joint Controller Agreement sets out what this arrangement encompasses.

22.6 The Black Pear application and interfaces to and from it will be managed by CAVUHB on behalf of the Joint Controllers, with each controller being a party to a Data Processor Agreement, including also appropriate contractual arrangements.

22.7 GP practices will continue to be the data controller for their own systems and will permit Black Pear to write data relating to clinics securely back to those systems.

22.8 Processor Activities

22.9 The data processor (Black Pear) will be contractually obliged to avoid responding to any privacy queries received for patients as though they are acting as a data controller. Any such queries should be immediately conveyed to the IG department of CAVUHB and to the patient's GP.

22.10 Security Measures

22.11 Access to systems at GP practices will be managed by Cluster / practice staff. Clinic staff will have individual logins and be provided with access to secure devices in order to retain control over access to data.

22.12 Additional Confidentiality Measure

22.13 Staff attending to deliver clinics will be reminded in writing as follows:

Respectful Reminder: Privacy Expectations

When secondary care staff are delivering clinics within a primary care setting, they may have access to information that they would not routinely have access to. This could include the electronic systems used by primary care, as well information held on paper or spoken by staff within Cluster / primary care premises.

Patients value the opportunity to receive diagnosis, treatment and support within their primary care practice. We want to do everything we can to reassure the public that their information will be treated with respect. Patients' human rights to privacy are important but it is appropriate to balance these rights with our respective legal obligation to deliver a safe and effective health service in the public interest.

Clinics delivered within primary care will be solely for the purpose of providing 'direct care'. This is defined as follows:

A. You work with an individual to provide health and / or social care services. This includes assessment, diagnosis, treatment, care management and service provision activities relating to an individual patient, *and* -

B. You have a legitimate professional relationship to any individual whose records you access i.e. they have been referred to the clinic you are providing .

Staff are respectfully reminded that where they do access patient information in the Cluster / practice, please:

- Remind your patient that their consultation will be shared with their GP
- Follow all relevant privacy and data protection policies of your own organisation
- Treat information from other organisations with the same confidentiality and respect as you would treat your own organisation's information.
- Access only the information that is necessary for you to carry out your work.
- Remain responsible for your own professional judgment based on any information you access.

Hopefully, that way we can retain the trust and confidence and trust of our patients.

We also remind you that your use of information systems is monitored routinely. Misuse of information systems can result in disciplinary, professional and criminal repercussions.

23 Appendix D – Signatories

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

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

Partner Organisation	Cardiff and Vale University Health Board	**Partner Organisation**	**[List of GP practices]**
Name		**Name**	
Position		**Position**	
Date		**Date**	
Signature		**Signature**	

Partner Organisation		**Partner Organisation**	
Name		**Name**	
Position		**Position**	
Date		**Date**	
Signature		**Signature**	

[Insert additional tables if required]

23.1**Appendix E**

Black Pear Secure Password Implementation

The login system enforces a timeout mechanism to prevent brute-force attacks and enhance security. The timeout duration increases based on the number of consecutive failed login attempts. After 3 failed attempts the lockout imposes a delay of 5s on every attempt. After 10 attempts, the delay increases to 20s per attempt.

Criteria used:

The criteria for a strong password are determined by the strengthify library, which uses the zxcvbn.js library for password strength evaluation. The specific strength requirement in the code is:

- A strength score of at least 4: This is explicitly mentioned in the validateForm function, where the form will only pass validation if the password's strength score is greater than or equal to 4.

Criteria for Password Strength (zxcvbn.js)

The zxcvbn.js library scores passwords on a scale of 0 to 4, where:

- 0: Too weak (e.g., common passwords or easily guessable patterns).
- 1: Weak.
- 2: Fair.
- 3: Good.
- 4: Strong.

To achieve a score of 4, passwords typically follow these characteristics:

1. Length: At least 12–16 characters long.
2. Complexity: A mix of:
    - Uppercase letters.
    - Lowercase letters.
    - Numbers.
    - Special characters (e.g., !, @, #, $, %).
3. Unpredictability: Avoid:
    - Common words or phrases (e.g., password, 123456).

- Patterns (e.g., abc123, qwerty).
- Repeated sequences (e.g., aaaa, 123123).
- Personal information (e.g., your name, birthdate).

4. Dictionary Resistance: The password should not appear in common password dictionaries or leaked databases.

Implementation Notes

The strengthify plugin provides real-time feedback about the password's strength as the user types.

The password field's appearance changes dynamically based on the strength of the entered password.

Validation Process

1. Users must input a password in the Password field.
2. If the user presses "Suggest password," a strong, system-generated password is automatically inserted into the form.
3. The form submission (onsubmit) will check if the password's strength score is at least 4 (unless the "Suggest password" button was used).
4. Password confirmation is also required to match the original password.