Cefnogir gan
Lywodraeth Cymru
Supported by
Welsh Government

Wales Accord on the Sharing of Personal Information

Data Processing Agreement:

Clinical In-Reach to Cluster Practices

Version Final 1.01

Review Date [31/12/2025]

Issue date [30/12/2024]

Internally assured on [Insert date here]

Template developed in partnership with

BLAKE MORGAN

Further information on how a Data Processing Agreement should be developed is contained within the

Guide on the Development of a Data Processing 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 DPA development has commenced

Where a processor carries out processing of personal data on behalf of a controller, Article 28(3) of the UK GDPR requires there to be a binding contract between the controller and the processor containing certain mandatory provisions.

A data processing agreement (DPA) is a contract signed between controllers and the processors that will handle their data and is intended to comply with the requirements of Article 28 of the UK GDPR.

A DPA sets out the nature, purpose and duration of the processing activities that will take place. It also specifies the types of personal data to be processed and the categories of individuals the data belongs to. It defines the rights and obligations the controller and processor will have.

Organisations who use the WASPI DPA template need to ensure that any completed DPA is legally binding from their own organisational requirements. WASPI provide a template agreement which can be used, but exclude all warranties and representations about the suitability of the document and exclude all liability in respect of the processing or contracts in place. 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.

This data processing agreement template has been prepared solely for the benefit of WASPI only. The template DPA was developed by WASPI in partnership with Blake Morgan LLP. Whilst other organisations may use this data processing agreement 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.

The template can be used for direct controller to processor activities or joint controller to processor activities.

DATA PROCESSING AGREEMENT

PART 1: FRONT SHEET

A. The Controller(s) identified below wish to engage the party whose details are set out below (the **Processor**) to carry out the processing activities described in this Front Sheet, and the Processor wishes to carry out those activities.

B. Both Parties acknowledge and agree that they have specific obligations under the Data Protection Legislation with respect to Personal Data.

C. This Agreement sets out the nature, purpose and duration of the processing activities that will take place and also specifies the types of personal data to be processed and the categories of individuals the data belongs to. It defines the rights and obligations the Controller and Processor will have and contains the mandatory clauses required by Article 28(3) of the UK GDPR.

D. This Front Sheet and the Terms and Conditions at part 2 (together, this **Agreement**) record the obligations of the Parties in respect of these processing activities.

E. Where there is a conflict between the provisions of this Front Sheet and the Terms and Conditions, then the provisions of this Front Sheet shall prevail.

I.	**Date of Agreement:**		23 day of December 2024
II.	**Controller(s)**	**Name**	Cardiff and Vale University Health Board and GP practices working within Clusters and delivering care to patients within Cardiff and the Vale of Glamorgan.
		Registered address	**Cardiff and Vale University Health Board:** University Hospital of Wales Heath Park Cardiff CF14 4XW
		Company number	N/A
		ICO registration number	Z1870171
		Point of Contact:	uhb.dpo@wales.nhs.uk
III.	**Processor:**	**Name**	Black Pear Software Ltd
		Registered address	60 Holborn Viaduct London EC1A 2F
		Company number	07030656
		ICO registration number	ZA215442
		Point of Contact:	07903 740 529
IV.	**Subject matter of the processing:**		Data is processed to enable the Controllers to share a view of the GP clinical record for the purposes of

<table>
<tr><td></td><td></td><td colspan="4">direct care and treatment and subsequently record clinic outcome data gathered by clinic providers, and to securely convey that data by a write back functionality into the clinical record to the GP Practice that has referred patients to the cluster clinic.</td></tr>
<tr><td>V.</td><td>Nature of the processing:</td><td colspan="4">Data is gathered by clinicians about patients attending centralised cluster clinics within the GP / Cluster practice. This data is gathered in a web app created by CAVUHB (Controller).which will allow view of the GP clinical record.

The data is passed securely by the web app to the Black Pear solution. The Black Pear solution will then securely send the information to the GP’s information systems.

CAVUHB will securely download clinic data from the Black Pear solution at quarterly intervals.

Black Pear will retain audit trails of clinician, patient and data content (for the duration of the contract).

CAVUHB will securely download audit records from the Black Pear solution on a monthly basis.</td></tr>
<tr><td>VI.</td><td>Purpose of the processing</td><td colspan="4">The purpose of the processing is for the Local Health Board to provide support and assistance to primary care providers in line with the National Health Service (Wales) Act 2006, Section 53. Allowing a shared access view to treating clinicians of the GP record to aid direct care and treatment.
The processing is also intended to facilitate the requirements of the relevant data standard notification to ensure that GPs are made aware of the outcomes of any clinic appointments.</td></tr>
<tr><td>VII.</td><td>Duration of the processing:</td><td colspan="4">The processing will commence on 2 January 2025 and continue for the duration of the contract to end of March 2027.</td></tr>
<tr><td>VIII.</td><td>Categories of Data Subject</td><td colspan="4">Patients attending clinics provided within Cluster / primary settings by secondary care clinicians.</td></tr>
<tr><td>IX.</td><td>Personal Data Processed as part of this Agreement:</td><td colspan="4">Name, date of birth and address to ensure the correct patient record is being viewed, updated and provided back to GP.
Some GP information is exposed to secondary care clinicians during clinic.
Details of observations, assessments, test results and treatment of individual patients for mental or physical health problems.</td></tr>
<tr><td rowspan="2">X.</td><td rowspan="2">Sub-processors</td><td>Name</td><td>Registered Address</td><td>Company number</td><td>ICO number</td></tr>
<tr><td>AMAZON WEB SERVICES EMEA SARL, UK BRANCH</td><td>1 Principal Place, London, Worship</td><td>BR019315</td><td>ZA481902</td></tr>
</table>

			Street, EC2A 2FA[i]		
XI.	**Minimum limit of insurance pursuant to clause 14.2**	£5m in aggregate.			
XII.	**Security Details**	Personal data will be accessed only using **Cluster / practice devices** and only **while clinic takes place** in Cluster / GP practice location. **Access** to the web app will be controlled by Cluster management / administration staff. **Secure encrypted connections** will be used to pass information:- • From GP system to Black Pear (and vice versa) • From Black Pear to web app (and vice versa) Existing mandatory **training** for all practice and health board staff provide sufficient knowledge about security but they will also be presented with the **supplementary** information shown at Appendix A. Data will not be recorded or held in paper format – the process is wholly electronic. Access to the web app will only be possible via strong password in the first instance while MFA is established during 2025. Users log onto their MFA-authenticated devices using their NHS logins. Users of Black Pear are authenticated using Black Pear's secure BP Auth service using a unique user identity (the user's 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 10^{10} 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. See Appendix B for details of the password policy that will be used. Data will be requested and presented via TLS using a secure API employing AES-256 encryption. The web app will be hosted on CAVUHB Servers and appropriate patching will be carried out by Microsft			

[i] The UK Branch of AWS is described here per address and company number. The ICO register details are for the parent company based in Luxembourg. No data is processed outside the UK region and the UK branch is listed as an alternate name of the parent company.

		365 Team in CAVUHB. Penetration testing and security vulnerabilities testing will take place annually. Black Pear carry out all required patching and at least annual penetration testing and annual vulnerability testing. Data encryption throughout will be to AES 256 standard. Data will not leave the United Kingdom.
XIII.	**Plan for return and/or destruction of the Personal Data once the processing is complete (*unless* required by law to retain the Data)**	Clinic data held by Black Pear will be downloaded at quarterly intervals by CAVUHB and subsequently deleted by Black Pear. Following the final download, Black Pear will certify destruction of all personal data within 3 months of the end of the contract. Audit records will be downloaded at quarterly intervals by CAVUHB and will be held by Black Pear until 30 June 2027.

This Agreement has been entered into on the date stated on the Front Sheet.

Signed for and on the behalf of the Controller(s)

Signature : .....

Name : .....

Position : .....

Date : .....

Signed for and on the behalf of the Processor

Signature : .....

Name : .....

Position : .....

Date : .....

PART 2: TERMS AND CONDITIONS

1. Definitions

1.1 In this Agreement the following terms shall have the following meanings:

1.1.1 **Data** means all data that is provided by the Controller(s) to the Processor, including Personal Data, and which is processed under this Agreement;

1.1.2 **Data Loss Event** any event that results, or may result, in unauthorised access by or disclosure to unauthorised third parties of the Personal Data held by the Processor under this Agreement, and/or actual or potential loss, damage, corruption and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach;

1.1.3 **Data Protection Legislation** means all applicable laws, regulations and regulatory rules which govern the processing of personal data and privacy including but not limited to (i) the Data Protection Act 2018 (ii) the UK GDPR (and to the extent it applies the EU GDPR) (iii) the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended) (iv) any subsequent legislation enacted and duly in force from time to time relating to the processing of Personal Data and (v) all guidance and / or codes of practice issued from time to time by the Information Commissioner or relevant government department, and any relevant rulings from time to time of the Information Commissioner or of the Courts of England and Wales relating to the processing of Personal Data;

1.1.4 **Data Subject Request** means a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to Data Protection Legislation to access their Personal Data;

1.1.5 **EIRs** the Environmental Information Regulations 2004, together with any guidance and/or codes of practice issued by the ICO or any relevant government body in relation to such regulations.

1.1.6 **FoIA** means the Freedom of Information Act 2000 and any subordinate legislation made under that Act from time to time, together with any guidance and/or codes of practice issued by the ICO or any relevant government body in relation to such Act;

1.1.7 **ICO** means the UK's Information Cmmissioner Office (or such organisation which may replace such

1.1.8 **Information** shall have the meaning given under section 84 of the FoIA and/or Regulation 2 of the EIRs;

1.1.9 **Party** shall refer to each of the Controller(s) and Processor who together shall be known as the **Parties**

1.1.10 **Personal Data**, **Data Subject**, **process**, **Personal Data Breach, Joint Controller(s)** and **Processor** have the meanings given in the Data Protection Legislation;

1.1.11 **Processor Personnel** means all directors, officers, employees, agents, consultants and contractors of the Processor and/or of any Sub-Processor engaged in the performance of its obligations under this Agreement ;

1.1.12 **Purpose** means the purpose set out in the Front Sheet.

1.1.13 **Request for Information** has the meaning set out in section 8 of the FoIA and/or Regulation 5 of the EIRs and includes any apparent request for such Information;

1.1.14 **SCCs** means (i) the ICO's International Data Transfer Agreement for the transfer of personal data from the UK and/or (ii) the ICO's International Data Transfer Addendum to EU Commission Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 as set out in the Annex to Commission Implementing Decision (EU) 2021/914 or such alternative clauses as may be approved by the UK from time to time;

1.1.15 **UK GDPR** and **EU GDPR** are as they are defined in section 3(10) of the Data Protection Act 2018; and

1.1.16 **Working Days** means Monday to Friday 09:00 to 17:00 excluding any statutory public holidays in Wales.

2. Appointment

2.1 In consideration of their compliance with their respective obligations under this Agreement, the Controller(s) appoints the Processor to process, and the Processor agrees to process, the Data for the Purpose and duration set out in the Front Sheet.

2.2 The Parties acknowledge that for the purposes of the Data Protection Legislation:

2.2.1 the Processor is a processor and Controller(s) are the controller(s) (and where there is more than one Controller they shall be Joint Controllers); and

2.2.2 the Controller(s) retain(s) control of the Personal Data and remains responsible for its compliance obligations under the applicable Data Protection Legislation.

2.3 The Front Sheet sets out the scope, nature and purpose of processing by the Processor, the duration of the processing, the types of Personal Data and categories of Data Subject.

2.4 The only processing that the Processor is authorised by the Controller(s) to do is listed in Front Sheet and may not be determined by the Processor.

2.5 All Parties will comply with all applicable requirements of the Data Protection Legislation. This Agreement is in addition to, and does not relieve, remove or replace, any Party's obligations under the Data Protection Legislation.

2.6 Without prejudice to the generality of clause 2.5, the Controller(s) will ensure that it has a valid legal basis in accordance with Article 6 of the UK GDPR to enable lawful transfer of the Personal Data to the Processor for the duration and purposes of this Agreement.

3. Obligations of the Processor

3.1 Without prejudice to the generality of clause 2, the Processor shall, in relation to the Data:

3.1.1 process Data only:

3.1.1.1 on the written instructions of the Controller(s) and only to the extent, and in such manner, as is necessary for the Purpose of the processing (as set out on the Front Sheet of this Agreement) in accorance with the Controller's written instructions. The Processor will not process the Personal Data for any other purpose or in a way that does not comply with this Agreement or the Data Protection Legislation; or

3.1.1.2 as required by the Data Protection Legislation or any other applicable law or any regulatory body. If the Processor is required by the Data Protection Legislation or any other applicable law or any regulatory bodyto process the Data, the Processor shall promptly notify the Controller before processing the Data unless prohibited by Law;

3.1.2 shall immediately inform the Controller(s) if it believes any instruction or processing is likely to breach any Data Protection Legislation or other applicable law;

3.1.3 not act in any way so as to cause the Controller(s) to breach of any of its obligations under the Data Protection Legislation;

3.1.4 comply promptly with any of the Controller(s)'s written instructions requiring the Processor to amend, transfer, delete or otherwise process the Personal Data, or to stop, mitigate or remedy any unauthorised processing;

3.1.5 at the written direction of the Controller(s) (and unless required by an applicable law to retain such Data), securely delete or return all Personal Data and copies thereof from all systems of the Processor (i) after the completion of the processing under this Agreement (ii) following termination or expiry of this Agreement or (iii) in any circumstance where the Controller is/are required to do so by the Data Protection Legislation, and provide written confirmation of this to the Controller(s). Where instructed to do so, the Processor must return all Personal Data to the Controller(s);

3.1.6 notify the Controller(s) immediately if the Processor or any of its employees, agents, sub-processors are requested to do any act which would infringe the Data Protection Legislation; and

3.1.7 maintain complete and accurate records and information to demonstrate its compliance with this clause 3 and make such records available on request to the Controller(s).

3.2 The Processor shall designate its own data protection officer if required by the Data Protection Legislation.

4. Security

4.1 The Processor must at all times ensure that it has in place appropriate technical and organisational measures to protect against unauthorised or unlawful processing, access, disclosure, copying, modification, storage, reproduction, display or distribution of Personal Data and against accidental or unlawful loss,destruction, alteration, disclosure of, or damage to, Personal Data.

4.2 The Processor must implement such measures to ensure a level of security which is appropriate to the harm that might result from the unauthorised or unlawful processing or accidental loss, destruction or damage of Personal Data. The measures in place shall ensure an appropriate level of security having regard to the nature of the Data to be protected, the risk involved, the state of technological development and the cost of implementing any measures.

4.3 Such measures shall include, but shall not be limited to, compliance with any Security Details set out in the Front Sheet.

5. Data Protection Impact Assessment

5.1 If so required by the Controller(s), the Processor shall provide all reasonable assistance to the Controller(s) in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistance may, at the discretion of the Controller(s), include:

5.1.1 a systematic description of the envisaged processing operations and the purpose of the processing;

5.1.2 an assessment of the necessity and proportionality of the processing operations;

5.1.3 an assessment of the risks to the rights and freedoms of Data Subjects; and

5.1.4 the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

6. Data Loss Event

6.1 The Processor shall immediately (and in any event within 24 hours of becoming aware of such Data Loss Event or potential Data Loss Event) notify the Controller(s) of any Data Loss Event or potential Data Loss Event.

6.2 Where the Processor becomes aware of Data Loss Event or potential Data Loss Event, it shall, without undue delay, also provide the Controller(s) with the following information:

6.2.1 description of the nature of the Data Loss Event, including the categories of in-scope Personal Data and approximate number of both Data Subjects and the Personal Data records concerned;

6.2.2 the likely consequences; and

6.2.3 a description of the measures taken or proposed to be taken to address the Data Loss Events including measures to mitigate its possible adverse effects.

6.3 Immediately following any Data Loss Event, the Parties will co-ordinate with each other to investigate the matter.

6.4 The Processor shall at its own cost and at no additional cost to the Controller(s) co-operate with the Controller(s), including:

6.4.1 assisting with any investigation;

6.4.2 providing access to the Processor's facilities, systems and Processor Personnel;

6.4.3 take reasonable and prompt steps to mitigate the effects and to minimise any damage resulting as a result of the Data Loss Event or otherwise required by the Controller(s); and

6.4.4 make available all relevant records, logs, files, Processor Personnel and other materials required to comply with Data Protection Legislation or reasonably required by the Controller(s).

6.5 The Processor's obligation to notify under clause 6.1 shall include the provision of further information to the Controller(s), as details become available.

6.6 The Processor shall not inform any third party or regulator of any such Data Loss Event without first obtaining the Controller(s)' prior written consent (except where required to do so by law).

6.7 The Processor agrees that the Controller(s) has the sole right to determine:

6.7.1 whether to provide notice of the Data Loss Event to any Data Subjects, the ICO, other regulators, law enforcement agencies or others, as required by law or regulation or in the Controller(s)'s discretion, including the contents and delivery method of the notice; and

6.7.2 whether to offer any type of remedy to affected Data Subjects, including the nature and extent of such remedy.

7. Data Subject Requests, complaints and third-party rights

7.1 The Processor shall assist the Controller(s) in, and take such technical and organisational measures as may be appropriate, and promptly provide such information to the Controller(s) as the Controller(s) may reasonably require, to enable the Controller(s) to:

7.1.1 comply with:

7.1.1.1 the rights of Data Subjects under Data Proetction Legislation, including responding to any Data Subject Requests; and

7.1.1.2 information or assessment notices served on the Controller(s) by the ICO or other relevant regulator under the Data Protection Legislation

7.1.2 ensure compliance with the Controller's obligations under the Data Protection Legislation with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators;

7.2 The Processor shall notify the Controller(s) immediately and in any case by the end of the next Working Day if it receives:

7.2.1 a Data Subject Request (or purported Data Subject Request);

7.2.2 a request to rectify, block or erase any Personal Data;

7.2.3 any other request, complaint, notice or communication that relates directly or indirectly to the processing of the Personal Data or to the Processor or Controller(s)'s compliance with the Data Protection Legislation;

7.2.4 receives a request from any third party for the disclosure of the Data (including where where compliance with such request is required or purported to be required by applicable law);

7.2.5 any communication from the ICO or any other regulatory authority in connection with Personal Data processed under this Agreement; or

7.2.6 fully co-operate and assist the Controller(s) in responding to any complaint, notice, communication or Data Subject request.

7.3 The Processor's obligation to notify under clause 7.2 shall include the provision of further information to the Controller(s), as details become available.

7.4 The Processor shall not respond to any complaint, communication or request made unless the Controller(s)' direct it to do so in writing.

7.5 The Processor shall provide the Controller(s) (at no additional cost to the Controller(s)) with full co-operation and assistance in relation to the Controller(s)'s obligations under Data Protection Legislation and any complaint, communication or request made (and insofar as possible within the timescales reasonably required by the Controller) including but not limited to promptly providing:

7.5.1 the Controller with full details and copies of the complaint, communication or request;

7.5.2 such assistance as is reasonably requested by the Controller to enable the Controller to comply with a Data Subject Request within the relevant timescales set out in Data Protection Legislation;

7.5.3 the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;

7.5.4 assistance as requested by the Controller with respect to any request from the Information Commissioner's Office, or any consultation by the Controller with the Information Commissioner's Office.

7.6 The Processor must not disclose the Personal Data to any Data Subject or to a third party other than in accordance with the Controller(s)'s written instructions, or as required by applicable law.

8. Sub-processors

8.1 The Processor is not permitted to subcontract any activity that will involve a third party processing the Personal Data without the Controller(s) prior written consent.

8.2 The Processor shall only authorise a third party (each a **"Sub-contractor"**) to process the Personal Data if:

8.2.1 the Controller(s) provide(s) prior written consent prior to the appointment of each subcontractor;

8.2.2 the Processor enters into a written contract with the subcontractor that contains terms substantially the same as those set out in this Agreement, in particular, in relation to requiring appropriate technical and organisational data security measures, and, upon the Controller(s) written request, provides the Controller(s) with copies of such contracts;

8.2.3 the Processor maintains control over all Personal Data it entrusts to the subcontractor; and

8.2.4 the subcontractor's contract terminates automatically on termination of this Agreement for any reason.

8.3 Those subcontractors approved as at the commencement of this Agreement are as set out on the Front Sheet.

8.4 The Processor must list all approved subcontractors in the Front Sheet, this includes any subcontractor's name and location and contact information for the person responsible for privacy and data protection compliance.

8.5 Where the subcontractor fails to fulfil its obligations under such written agreement, the Processor remains fully liable to the Controller(s) for the Sub-contractor's performance of its Agreement obligations.

8.6 On the Controller's written request, the Processor will audit a subcontractor's compliance with its obligations regarding the Controller's Personal Data and provide the Controller with the audit results.

9. International data transfers

9.1 The Processor shall not transfer any Personal Data outside of the UK or European Economic Area without the prior written consent of the Controller(s) (which may be withheld in its absolute discretion). Any transfer outside the European Economic Area shall also be subject to the Processor complying with Chapter 5 of the UK GDPR.

9.2 If any Personal Data transfer between the Controller(s) and the Processor requires execution of SCCs in order to comply with the Data Protection Legislation (where the Controller(s) is/are the entity exporting Personal Data to the Processor outside the Uk and EEA), the Parties will complete all relevant details in, and execute, the SCCs and take all other actions required to legitimise the transfer.

10. Confidentiality

10.1 The Processor shall ensure that all Personal Data is treated and maintained as confidential information and is not published, disclosed or divulged to any third party by the Processor or any of its employees, workers or contractors, unless directed in writing to do so by the

Controller(s) unless required by any applicable law, court or regulator (including the ICO). If any applicable law, court or regulator (including the ICO) requires the Procesor to process or disclose the Personal Data to a third party, the Processor must first inform the Controller(s) of such legal or regulatory requirement and give the Controller(s) an opportunity to object or challenge the requirement, unless the applicable law prohibits the giving of such notice.

10.2 The obligations placed on the Processor in this clause 3 will also apply to all non-personal data and the information contained within the Data. The Processor, its employees, servants, agents or sub-contractors accept this duty of confidentiality regarding all non-personal data.

10.3 The obligations relating to confidentiality set out in clause 10 shall survive termination or expiry of this Agreement.

11. Processor Personnel

11.1 The Processor shall:

11.1.1 ensure that Processor Personnel do not process Data except in accordance with this Agreement;

11.1.2 ensure that the Personal Data is not made available by default to all employees, workers or contractors of the Processor or any sub-contractor and only to such individuals as are strictly required in order to meet the obligations under this Agreement have access to the Personal Data; and

11.1.3 take reasonable steps to ensure the reliability and integrity of Processor Personnel who have access to the Personal Data;

11.1.4 ensure that any Processor Personnel authorised to process the Personal Data are:

11.1.4.1 are aware of and comply with the Processor's duties under this Agreement;

11.1.4.2 are subject to appropriate confidentiality undertakings with the Processor or any Sub-processor;

11.1.4.3 are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Controller or as otherwise permitted by this Agreement; and

11.1.4.4 have undergone adequate training in the use, care, protection and handling of personal data.

12. Rights of the Controller(s)

12.1 The Controller(s) is/are entitled, on giving not less than five (5) Working Days' notice to the Processor, to inspect, appoint representatives to inspect, or to permit regulators, auditors or the ICO (or their representatives) to attend, access and/or inspect all facilities, equipment, documents and electronic data relating to the processing of Data by the Processor under this Agreement. The Controller shall, and shall ensure that its officers, employees and representatives performing such inspection shall, keep everything discovered in respect of the inspection strictly confidential including so as to comply with all reasonable confidentiality requirements of the Processor.

12.2 Save in respect of a regulator (who shall be permitted unfettered access), the Controller(s) will carry out such audit during normal working hours.

12.3 The requirement to give notice under clause 12.1 will not apply if the Controller(s) reasonably believes that the Processor is in material breach of any of its obligations under this Agreement.

13. Term and termination

13.1 Unless terminated in accordance with clause 13.2, this Agreement shall continue in full force and effect until the completion of the processing activities set out on the Front Sheet and thereafter until all Personal Data has been securely deleted or returned to the Controller(s) in accordance with clause 3.1.5.

13.2 This Agreement may be terminated:

13.2.1 immediately by the Controller(s), if the Processor commits any breach of its obligations under this Agreement; or

13.2.2 at any other time by either Party on one month's prior written notice to the other Party.

14. Indemnity

14.1 The Processor must on an ongoing basis fully and effectively indemnify and hold harmless and defend at its own expense the Controller(s) against all claims, expenses, costs (including reasonable legal costs), damages, losses, demands and regulatory fines awarded against or incurred or paid by the Controller(s) arising as a result of the Processor's negligence or any breach of the terms of this Agreement.

14.2 The Processor shall insure against its liability under this clause 14 with a minimum aggregate limit of indemnity in the amount set out in the Front Sheet or such other sum as may be agreed between the Controller(s) and the Processor in writing.

14.3 For the duration of this Agreement, the Processor shall maintain employer's liability insurance in respect of the Processor's staff in accordance with any legal requirement for the time being in force.

14.4 Nothing in this Agreement excludes or limits the liability of either Party for:

14.4.1 death or personal injury caused by such Party's negligence;

14.4.2 fraud or fraudulent misrepresentation; or

14.4.3 any other liability which cannot lawfully be excluded or limited

15. Freedom of Information

15.1 The Processor acknowledges that the Controller(s) may be a public authority for the purpose of FoIA and/or EIRs.

15.2 The Processor shall:

15.2.1 notify receipt of any Requests for Information in connection with the Data to the Controller(s) as soon as practicable after receipt and in any event within two (2) Working Days of receiving a Request for Information and comply with any instructions provided by the Controller(s);

15.2.2 not respond directly to a Request For Information addressed to the Authority unless authorised in writing to do so by the Authority.

15.2.3 provide the Controller(s) with a copy of all Information in its possession or power in the form that the Controller(s) requires in connection with a Request for Information within five (5) Working Days (or such other period as the Controller(s) may specify) of the Controller(s) requesting that Information; and

15.2.4 provide all necessary assistance and cooperation as reasonably requested by the Controller(s) to enable the Controller(s) to comply with its obligations under the FoIA and EIRs within the time for compliance set out in section 10 of the FoIA or Regulation 5(2) of the EIRs;

15.3 The Processor acknowledges that the Controller(s) may be required under the FoIA and EIRs to disclose Information (including information about this Agreement itself or the services provided by the Processor) without consulting or obtaining consent from the Processor. The Controller(s) shall take reasonable steps to notify the Processors of a Request For Information (in accordance with the Secretary of State's section 45 Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the FoIA) to the extent that it is permissible and reasonably practical for it to do so but (notwithstanding any other provision in this Agreement) the Controller(s) shall be responsible for determining in its absolute discretion whether any Information and/or any other information is exempt from disclosure in accordance with the FoIA and EIRs.

15.4 The Processor acknowledges that the Controller(s) may publish basic details of the Agreement in the appropriate log under the Controller's Publication Scheme.

16. Miscellaneous

16.1 No variation of this Agreement shall be valid unless in writing and signed by, or on behalf of, each of the Parties.

16.2 The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Controller may upon giving the Processor not less than 30 Working Days' notice to the Processor amend this Agreement to ensure that it complies with any guidance issued by the Information Commissioner's Office.

16.3 Any notice given to a Party under or in connection with this **Agreement** must be in writing and delivered to the relevant Party's Point of Contact (as set out in the Front Sheet and as may be amended by the relevant Party by written notice to the other Party). This clause does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.

16.4 This Agreement constitutes the entire agreement between the Parties in respect of the processing of Personal Data described on the Front Sheet and supersedes and extinguishes all previous drafts, arrangements, understandings or agreements between them, whether written or oral, relating to the subject matter of this Agreement.

16.5 A person who is not a Party to this Agreement shall not have any rights under or in connection with it.

16.6 This Agreement, and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims), shall be governed by, and construed in accordance with the law of England and Wales as applied in Wales.

16.7 The Parties irrevocably agree that the courts of England and Wales sitting in Cardiff, shall have exclusive jurisdiction to settle any dispute or claim that arises out of or in connection with this Agreement.

Appendix A - Respectful Reminder: Privacy Expectations

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 the patient that your 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.

Appendix B - Black Pear Secure Password Implementation

1.1 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.

1.2 Criteria used:

1.3 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.

1.4 Criteria for Password Strength (zxcvbn.js)

1.5 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.

1.6 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.

1.7 Implementation Notes

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

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

1.10 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.