DATA ACCESS AGREEMENT

October 2019

Introduction
In general terms, Positive Life does not share personal information of its data subjects.

However in the event of a request, this Data Access Agreement (DAA) template should be completed where personal identifiable data is shared for a secondary purpose (e.g. not for direct care or for a reason other than the initial purpose for which the data was collected). 'Identifiable' means data which could lead to any individual being identified and includes pseudonymised data.
(See Section A)

It is important to consider what type of data meets the request and that Section A is completed before proceeding with this DAA.

Please also see Positive Life's

- Data Protection & Retention Policy
- Confidentiality Policy
- Managing Subject Access Requests
- Privacy Notice.

Completing this form

The form is divided into Sections (A-I) as detailed below:

Section A: Classification of data required
Section B: Title of Agreement and Details of Requesting / Commissioning Organisation(s)
Section C: Details of Identifiable Data Items required and rationale
Section D: Consent issues
Section E: Data Protection
Section F: Measures to prevent disclosure of Personal Identifiable Information
Section G: Data Retention
Section H: Declaration: Requesting Organisation
Section I: Declaration: Owner Organisation

Appendix 1: Data Destruction Notification
Appendix 2: Principles Governing Information Sharing
Appendix 3: Definitions
Appendix 4: Contact Details

Please ensure that the completed / signed form is returned to the relevant contact in each organisation (**see attached Appendix 4 for contact details**)

*******IMPORTANT*******

PLEASE REVIEW AND COMPLETE SECTION A BEFORE PROCEEDING

(A) Classification of data required		
Identifiable data	The data to be shared will contain Client Identifiable Details i.e. any of the following: Name, Address, Full Postcode, Date of Birth, Case-note Number or other unique identifier that would link the data to identifiable details	Yes ☐ Please complete ALL sections of this DAA
Pseudonymous data	The data to be shared will contain no personal identifiers (as described above); however a unique code or key will be included that allows the possibility of linking this in future to a specific data subject. The pseudonymisation process will be completed at source by Positive Life who alone will securely retain the key to re-identify the data.	Yes ☐ Please complete sections B, C, G and H of this DAA
Anonymous data	The data to be shared will contain **NO** identifiable data items (as described above). At no stage will any party be able to link the data to an identified or identifiable natural person.	Yes ☐ A DAA is not required

(B) Title of Agreement / Organisations to which the data will be shared

Title of Agreement	
Date of Request	

An update of an earlier extract ☐ New application ☐

Date Access to Begin: _____

Date Access Ends: _____

Review date if on-going agreement:_____

Details of Requesting Organisation	
Name of Requesting Organisation: Please note that the Data Access Agreement will be immediately returned unless the requesting organisation has signed section H.	
Name of Authorised Officer Requesting Access to Data (please print)	
Position/Status	
Address Postcode	
Sector of the requesting organisation e.g. Voluntary, Public, Private etc	
Telephone Number	
Email Address	
Name and Telephone Number of Organisation's Personal Data Guardian/Caldicott Guardian	

If you require the data to carry out work **on behalf of another organisation**, please complete the additional Table below. If not, please go straight to section (C).

Commissioning Organisation (if relevant)	
Name of Commissioning Organisation	
Contact Name	
Title	
Contact Number	
Email Address	

(C) Details of Identifiable Data Items required and rationale	
Please provide a list of the identifiable data being requested (see section A for examples)	Please indicate the reasons for requiring each of these data items
1 _____ 2_____ 3 _____ 4_____ 5_____ 6_____ 7_____ 8_____ 9_____ 10_____ Continue on separate sheet if necessary	1_____ 2 _____ 3_____ 4 _____ 5_____ 6 _____ 7_____ 8 _____ 9_____ 10_____ Continue on separate sheet if necessary

Processing of information	
Please state in as much detail as possible the purpose for which the data is required and how it will be processed once received. Please include details of any record linking or matching to other data sources. *(please continue on a separate sheet if necessary or attach any relevant documentation)*	
System(s) from which data is to be extracted (if known) for e.g. Advice-Pro etc. Please also include sites or geographical locations (if known)	
Frequency of transfers (*Please Tick*)	Once ☐ Other ☐ (Please specify) _____

(D) Consent Issues	
If you are requesting personal identifiable/sensitive data for secondary purposes, there is an expectation that you will have explicit written consent from the service user(s) to access their information. Consent means offering individuals genuine choice and control. This will require a very clear and specific statement of consent, which should be in writing and held on the service user's file. It should be clear to the individual what they are consenting to and who will have access to their information. It should be easy for individuals to withdraw consent and they should be made aware that they can do this at any time.	
Do you have the individual's consent?	Yes ☐ No ☐
If yes, please provide a copy of the Consent Form	Consent Form attached - Yes ☐ *(if Yes, proceed to section E)*
If no, why have you not been able to obtain consent?	
If no consent, what other lawful basis are you relying on to obtain the data? *(please consult DP legislation or discuss with your Data Protection Officer)*	
In the absence of consent or any other lawful basis, it will only be appropriate to share anonymous data or pseudonymous data (data pseudonymised at source). Please indicate which is required.	I require anonymous data only ☐ *(no DAA required)* I require pseudonymous data ☐ *(proceed to complete the declaration at section H)*

(E) Data Protection (of Requesting Organisation)	
Do you have a confidentiality / privacy policy which complies with Data Protection legislation?	Yes ☐ No ☐
Are confidentiality clauses included within contracts of all staff with access to the person identifiable information?	Yes ☐ No ☐
Are all staff trained and aware of their responsibilities under Data Protection legislation and adhere to the Data Protection Principles?	Yes ☐ No ☐
Provide details /copy of your ICT security policy	
You must be registered with the Information Commissioner's Office (ICO) to process personal data. Please provide your ICO registration number	
Have you conducted a Privacy Impact Assessment?	Yes ☐ No ☐ If yes please include a copy with this form.

(F) Measures to Prevent Disclosure of Person Identifiable Information (of Requesting Organisation)	
Is the data to be viewed only (v); or Viewed and updated (U); or Transferred and Viewed (T)?	Please specify: _____
How will the information provided be securely transferred to your organisation?	
Describe the physical security arrangements for the location where **person identifiable data** is to be: - processed; and - stored (if different to above).	
Will this data be accessed or transferred by you to another organisation?	Yes ☐ No ☐ (If Yes, please give details including in what country it will be stored)
If applicable, how will you secure information provided being transferred by you to another organisation?	
Is a separate agreement in place to ensure the security of the data held by the 3rd party?	Yes ☐ No ☐

System Information	
Provide details of access and/or firewall controls implemented on the system, and measures to encrypt which are in place.	

(G) Data Retention (of requesting Organisation)	
Please state the date by which you will be finished using the data. If this is not applicable you need to explain why?	
If the data retention period is greater than two years, please indicate the reasons for this. (**The maximum data retention period is 2 years, after this time a review of this agreement is required**)	
Describe the method of data destruction you will employ when you have completed your work using person identifiable data	

When appropriate, please ensure that the Data Destruction Notification (Appendix 1) is completed within the specified retention period and returned to the appropriate contact person (see Appendix 4).

(H) Declaration: Requesting Organisation

Data Protection Undertaking on Behalf of the Organisation Wishing to Access the Data

My organisation requires access to the data specified and will conform to Data Protection legislation; the Information Commissioner's Data Sharing Code of Practice; and the guidelines issued by the Department of Health in January 2012 in *"The Code of Practice on Protecting the Confidentiality of Service User Information".*

I confirm that the information requested, and any information extracted from it,

- Is relevant to and not excessive for the stated purpose
- Will be used only for the stated purpose
- Will be stored securely
- Will be held no longer than is necessary for the stated purpose
- Will be disposed of fully and in such a way that it is not possible to reconstitute it
- That all measures will be taken to ensure personal identifiable data will not be disclosed to third parties
- Where appropriate, the Health and Social Care organisation will be informed of the identifiable data being deleted / destroyed (see Appendix 1)
- In the case of pseudonymised data, the process of de-identifying data will be completed at source. The key to re-identification will be held only by the Trust and at no stage will the data we receive be attributed to an identified or identifiable natural person

I *(name:printed)* _____, as the Authorised Officer of

(Organisation) _____, declare that I have read and understand my obligations and adhere to the conditions contained in this Data Access Agreement.

Signed: _____

(Personal Data Guardian)

Signed: _____

(IAO/SIRO)

Date: _____

(I) Declaration – Positive Life

DATA ACCESS AGREEMENT

I CONFIRM THAT:

1. The _____
consents to the disclosure of the data specified, to the organisation identified in Section B of this form.

   The disclosure of the data conforms to the guidelines issued by the Department of Health Code of Practice on Protecting Confidentiality of Service User Information, January 2012; and the Information Commissioner's Data Sharing Code of Practice.

Signed: _____ *(Trust internal use)*
(Information Governance and / or ICT Security)

Signed: _____
(Personal Data Guardian) OR (Senior Information Risk Owner SIRO)

Date: _____

Please note that this organisation has the right to inspect the premises and processes of the requesting organisation to ensure that they meet the requirements set out in the agreement.

Any loss, theft or corruption of the shared data by the requesting organisation must be immediately reported to the Personal Data Guardian of the owning organisation. Please also note that any serious breaches, data loss, theft or corruption should also be reported to the ICO by the Data Controller.

Appendix 1

Data Destruction Notification

(to be completed on all occasions when data is transferred external to Positive Life)

Authorised users of the person identifiable data have, under the terms and conditions of the Data Access Agreement, a requirement to destroy the data on or before the retention date stated in Section (H).

This form should be completed on destruction of the data and returned to the Personal Data Guardian.

This form should be completed on destruction of the data, and returned to the relevant Trust contact (see Appendix 4):-

Data Destruction Notification	
Name of Organisation	
Name of Authorised Officer (please print)	
Position/Status	
Address	
Telephone Number	
Mobile Number (Optional)	
Fax Number	
Email Address	
Title of Agreement	
Date Declaration Signed	
Date Data Received	
Date Data Destroyed	

Signature	
Date	

Appendix 2 - Principles Governing Information Sharing[1]

Code of Practice 8 Good Practice Principles[2]	DPA 1998 Principles[4]	GDPR Principles[4]	Caldicott Principles[3]
1. All organisations seeking to use confidential service user information should provide information to service users describing the information they want to use, why they need it and the choices the users may have. **2.** Where an organisation has a direct relationship with a service user then it should be aiming to implement procedures for obtaining the express consent of the service user. **3.** Where consent is being sought this should be by health and social care staff who have a direct relationship with the individual service user. **4.** 'Third Party' organisations seeking information other than for direct care should be seeking anonymised or pseudonymised data. **5.** Any proposed use must be of clear general good or of benefit to service users. **6.** Organisations should not collect secondary data on service users who opt out by specifically refusing consent. **7.** Service users and/or service user organisations should be involved in the development of any project involving the use of confidential information and the associated policies. **8.** To assist the process of pseudonymisation, the Health and Care Number should be used wherever possible.	**1.** Data should be processed fairly and lawfully. **2.** Data should be processed for limited, specified and lawful purposes and not further processed in any manner incompatible with those purposes. **3.** Processing should be adequate, relevant and not excessive. **4.** Data must be accurate and kept up to date. **5.** Data must not be kept longer than necessary. **6.** Data must be processed in line with the data subject's rights (including confidentiality rights and rights under article 8 of the Human Rights Act). **7.** Data must be kept secure and protected against unauthorised access. **8.** Data should not be transferred to other countries without adequate protection.	**1.** processed lawfully, fairly and in a transparent manner **2.** Purpose limitation - collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes **3.** Data minimisation - adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed **4.** Data Quality - accurate and, where necessary, kept up to date **5.** Storage Limitation - kept for no longer than is necessary. **6.** Integrity and Confidentiality - processed in a manner that ensures appropriate security of the personal data Principles relating to individuals' rights and overseas transfers of personal data are specifically addressed in separate GDPR articles.	**1.** Justify the purpose(s) for using confidential information. **2.** Only use it when absolutely necessary. **3.** Use the minimum that is required. **4.** Access should be on a strict need-to-know basis. **5.** Everyone must understand his or her responsibilities. **6.** Understand and comply with the law. **7.** The duty to share information can be as important as the duty to protect patient confidentiality

[1] These principles must be followed by health and social care organisations when considering use and disclosure of service user information.
[2] Code of Practice, paragraph 3.17.
[3] PDG Principles are adopted from the Caldicott Principles (revised September 2013) established in England and Wales.
[4] GDPR Principles apply from 25th May 2018 replacing the Data Protection Act 1998 (DPA)

Appendix 3 - Definitions

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;

Consent
'Consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

Processing
'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;

Pseudonymisation
'Pseudonymisation' 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 natural person;

Data Controller
'Controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

Data Processor
'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

Third party
'Third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

Appendix 4 - Contact details

Positive Life
Corporate Services Manager / Data Protection Officer
20 Derryvolgie Avenue
Belfast
BT9 6FN
Email: paula@positivelifeni.com
Tel: 028 9024 9268