DATA ACCESS AGREEMENT

Personal Identifiable Data for Non-Direct Care Purposes

Introduction

All Health and Social Care organisations (HSC) must ensure that when sharing HSC data for non direct care (secondary purposes), assurances are provided by the requesting organisations that they comply with the Data Protection Act (1998) and that they have relevant DPA Policies and Procedures in place which their staff are aware of.

Researchers undertaking studies and who require access to patient identifiable information and / or anonymous HSC data should follow the research protocol (Research Governance Framework for Health and Social Care in Northern Ireland.

The following Data Access Agreement must be completed by any organisation wishing to access HSC Trust data. It must be considered for approval and signed by the supplier organisation's Personal Data Guardian

It is essential that <u>ALL</u> sections of this document (except section I (declaration – owner organisation)) are completed by the requesting organisation. Failure to do so will result in the document being returned to you for completion. Your request for access to data cannot be processed until the owner organisation is in possession of all information requested.

Please refer to Appendix 2, 'Principles Governing Information Sharing' for guidance.

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

Section A: Details of Requesting Organisation
Section B: Commissioning Organisation
Section C: Details of data items requested
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

Please ensure that this form is returned to the Data Protection Officer:

<Name>
<Email>
<Telephone>

Internal Reference: _____

Title of Agreement	
Date of Request	

Please state if this is an update of a previous agreement or a new request for personal identifiable information

An update of an earlier extract ☐ New application ☐

(A) Details of Requesting Organisation	
Name of Requesting Organisation:	
Name of Authorised Officer Requesting Access to Trust Data (please print)	
Position/Status	
Address Postcode	
Telephone Number	
Email Address	
Name and Telephone Number of Requesting Organisation or Personal Data Guardian	

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

(B) Commissioning Organisation	
Name of Commissioning Organisation	
Contact Name	
Title	
Contact Number	
Email Address	

(C) Details of 'Data Items' Required:	
Please provide a list and description of the data to which the request applies, eg include all identifier attributes, (eg Name, Address, Postcode, Date of Birth, Gender, HSC Number, Diagnosis Code, Religion etc)	
1._____	6. _____
2. _____	7. _____
3. _____	8. _____
4. _____	9. _____
5. _____	10. _____

Please state in as much detail as possible, the purpose for which the data are required by the organisation named in section (A) including any record linking or matching to other data sources. Please continue on a separate sheet if necessary or attach any relevant documentation.

Justification of Purpose	
Please indicate how you propose to process the data once received (eg to extract and anonymise Service User information; for auditing and monitoring of Service User care and treatment.	

System(s) from which Data is to be extracted (If Known) Please include sites or Geographical locations (If Known)	
For example PAS, Ulster Hospital	
Is the Data to be Viewed only (V); or Viewed and Updated (U); or Transferred and Viewed (T)?	Please specify: _____
Will Data contain Client Identifiable Details?	**(Please Tick)** Yes ☐ No ☐
Frequency of transfers	Once Only ☐ Other ☐ (Please specify) _____

(D) Consent Issues	
Do you have the individuals' consent?	Yes ☐ No ☐
If no, why is it not practical to obtain consent?	
Have you involved the individual(s) concerned?	

(E) Data Protection	
Do you have a confidentiality / privacy policy which complies with the Data Protection Act 1998?	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 the Data Protection Act 1998 and adhere to the eight Data Protection Act Principles?	Yes ☐ No ☐

(F) Measures to Prevent Disclosure of Person Identifiable Information	
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)
How will you secure the information provided being transferred?	
Provide details/copy of the ICT security policy for your organisation.	

Provide confirmation that your organisation has Data Protection notification for purposes of analysis.	
Describe the physical security arrangements for the location where person identifiable data is to be: – processed; and	
– stored *(if different to above).*	

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	
Please state the date by which you will be finished using the data.	
If the retention period which you require the data is greater than one year, please indicate the reasons. (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.	

Please ensure that the Data Destruction Notification (Appendix 1) is completed within the specified retention period and returned to the Personnel Data Guardian.

(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 the Data Protection Act 1998 and the guidelines issued by the DHSSPS Executive in January 2009 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.
- The Health and Social Care organisation will be informed of the data being deleted / destroyed.

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: _____

(Authorised Officer)

Date: _____

Signed:

_____

(Personal Data Guardian)

Date:

_____

(I) Declaration – Owner Organisation

DATA ACCESS AGREEMENT

I CONFIRM THAT:

1. ********* Health and Social Care organisation consents to the disclosure of the data specified, to the organisation identified in Section A of this form.
   The disclosure of the data conforms to the guidelines issued by the DHSSPS NI Code of Practice on Protecting Confidentiality of Service User Information, 2009.

2. The data covered by this agreement are: **(*delete as appropriate)**

   - Either data which are exempt from the Data Protection Act 1998, or
   - Are notified under the Data Protection Act 1998 and their disclosure conforms to the current notification under The Act.

Signed: _____

(Personal Data Guardian)

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.

Appendix 1

Data Destruction Notification

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:-

ADDRESS

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 Principles	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.** 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.

[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 established in England and Wales.