INFORMATION SHARING AGREEMENT

Between

# UCL SLMS (‘the Processor’)

and

**[Full name of Organisation] (‘the Data Controller’)**

|  |  |
| --- | --- |
| **Document Information** | |
| **Document Name** | SLMS-IG22 UCL DP ISA |
| **Author** | Shane Murphy |
| **Issue Date** | 02/08/2013 |
| **Approved by** | Chair of SLMS IGSG |
| **Next review** | One year |

|  |  |  |
| --- | --- | --- |
| **Document History** | | |
| **Version** | **Date** | **Summary of change** |
| 0.1 | 05/04/2013 | First draft for discussion |
| 0.2 | 10/05/2013 | Second draft included comments from Tito Castillo |
| 0.3 | 20/06/2013 | Third draft for discussion included comments from UCLP |
| 1.0 | 02/08/2013 | Approved by Chair of SLMS IGSG |

|  |
| --- |
| This document is subject to an annual review by SLMS IGSG. |

**Compliance with the Data Protection Act 1998**

Under the terms of [this/an] agreement between the UCL SLMS and the Data Controller dated [date], the Processor provides [describe the services]for the processing of personal data under the Data Controller’s control. For the avoidance of doubt, in relation to the Data Protection Act 1998, it is accepted by both parties that UCL SLMS is operating as the Data Processor and the [Name of Organisation] as a Data Controller. The personal data transferred under this Agreement is:

**[Describe personal data to be transferred]**

UK law does not permit the Data Controller to allow the Processor to process such personal data unless the Data Controller complies, and can demonstrate that the Data Controller complies, with certain requirements as set out in the seventh Data Protection principle. This agreement places obligations on the Data Controller and the Processor to discharge their respective obligations under the Data Protection Act 1998 (‘the Act’).

1. Security

The Processor will take appropriate technical and organisational measures against unlawful and unauthorised processing of personal data and against accidental loss, destruction of and damage to the personal data. In particular, the Processor is required to:

keep the personal data private and confidential by secure transfer such as N3 and/or AES 256 bit encryption; pseudonymisation, anonymisation or other information security techniques agreed between the parties;

using all reasonable endeavours minimise disclosure of the personal data to third parties to the fullest extent possible by use of techniques and controls mentioned in sections 1.1 and 1.3 of this agreement;

allow access to the personal data on a ‘need to know’ basis and use appropriate technical and organisational controls to ensure this requirement is satisfied;

ensure that any recipients of the personal data are subject to a binding duty of confidentiality in relation to the data.

1. Personnel

The Processor will ensure the reliability of all of its personnel (whether employees or contractors) that may have access to the personal data and to ensure that they are adequately trained in the processing of personal data. If the Processor’s staff are in breach of any of the aforementioned technical and organisational controls they will be subject to the Processor’s disciplinary procedures. [For the avoidance of doubt the Data Controller will have the authority to demand that the Processor’s staff concerned, subject to any acceptable re-training, do not have any further access to the Data Controller’s personal data.]

1. Purposes and procedure for Sharing Information

It is accepted that the personal data is provided for the purpose of Non Healthcare Medical purpose (aka secondary use) and therefore each party will act in

accordance with the requirements contained in Connecting for Health document NPFIT-FNT-TOBPR-0023.01, “Pseudonymisation Implementation Project (PIP) Reference Paper 1, Guidance on Terminology” dated 20/11/2009, in relation to the personal data and will only use the personal data to provide the services under this Agreement. See Appendix 1. The Data Controller shall complete Appendix 3, of this Agreement, to acknowledge they have assessed basic requirements of the ICO Data Sharing Code of Practice.

The Processor will act in accordance with the Data Controller’s instructions in relation to the personal data and will only use the personal data to provide the services under this Agreement and for no other purposes unless agreed by an addendum to this agreement. The parties have an obligation of mutual transparency towards each other and members of the public. This it is acknowledged is discharged through their respective Publication Schemes under the Freedom of Information Act. The purpose(s) for which the Processor may use the personal data are as follows:

**[Describe purpose(s)]**

and for no other purpose.

* 1. The Data Controller will use all reasonable endeavours to provide the Data Processor with pseudonymised data. All due care will be discharged by the Data Controller to ensure that the pseudonymised data, whether alone or when processed together with other information in possession of either party, or another party is not capable of being re-identified as personal data. For the avoidance of doubt all due care will be represented by the requirements of the Information Commissioner’s “Re-identification testing” and the ”motivated intruder test” as specified in the Anonymisation: Managing Data Protection Risk Code of Practice published in November 2012. The Data Controller will implement these requirements by exercising all due care considered necessary for the processing of sensitive personal data.
  2. Where it is not possible to use effectively anonymised information, consent from service users may be required. The parties acknowledge that any disclosure without consent will need to be fully considered to ensure compliance with the law.

3.3 Any information transmitted outside of the Data Processor’s IDHS shall not contain personal data. The information will be effectively anonymised or pseudonymised.

3.4 It is expressly forbidden to disclose any personal data, or sensitive personal data to a third party unless this has been authorised by a duly authorised and responsible officer of the Data Controller.

1. Subcontractors

Subcontract of any activity involving a third party processing the personal data is not permitted without the Data Controller’s prior written consent.

1. Transferring personal data outside the European Economic Area

The transfer of personal data to any territory outside the European Economic Area is not permitted without the Data Controller’s prior written consent and suitable assurances that the informed consent, where applicable, of data subjects has been obtained.

1. Providing assistance

6.1 The Processor will assist the Data Controller promptly with all subject access requests which may be received from individuals whose personal data the Processor is processing on behalf of the Data Controller;

6.2 The Processor will promptly amend, transfer or delete any personal data that the Processor is processing for the Data Controller if the Data Controller requires the Processor to do so;

6.3 The Processor will notify the Data Controller immediately of all communications the Processor receives from any person which suggests non-compliance with the Act and the Processor will not do anything or enter into any communication about it unless the Data Controller expressly authorises the Processor to do so;

6.4 The Processor will provide the Data Controller with a copy of the personal data as soon as possible if the Data Controller asks the Processor to do so in the format and on the media which is specified in the Data Controller’s reasonable request;

6.5 The Processor will promptly inform the Data Controller of any breach or suspected breach of the Data Protection Act involving the Data Controller’s personal data.

6.6 The Processor will promptly inform the Data Controller of any information security

incident or suspected information security incident involving the Data Controller’s

personal data.

1. Audit

The Processor will permit the Data Controller to monitor compliance with the terms of this agreement, which may involve the Data Controller or its nominated representative coming onto any premises where the personal data are being processed with at least 10 working days’ notice.

1. Ending this arrangement

Either party may end this arrangement by giving one month's written notice to the other. However, this notice period will be reduced so that it ends with immediate effect if the reason for ending the arrangement is because:

a resolution is passed or an order is made for the other to be wound up (other than for a solvent amalgamation or reconstruction);

the other becomes subject to an administration order or a receiver or administrative receiver is appointed;

somebody with a right to do so takes possession of any of the other's property or assets in the event of it being dissolved; or

the other ceases to carry on business in the United Kingdom.

8.5This arrangement will end automatically upon termination or expiry of the Agreement (for whatever reason). When this arrangement ends, unless otherwise agreed, the Processor will return [or securely delete/destroy] all of the Data Controller’s personal data in their possession and provide written warranty of its actions.

8.6 The Data Controller will be entitled to end this arrangement immediately on written

notice if the Processor is found to have breached the Act, or the Processor’s

actions have led to the compromise of the Data Controller’s personal data in any way. However, the Data Controller will provide all reasonable opportunity for the Data Processor to rectify the breach or incident and provide reasonable assistance to mitigate the impact of the incident prior to issuing the written notice.

9 Transferring this arrangement

This arrangement is personal to the Processor and is not permitted to assign or transfer any of your rights or obligations in it without the Data Controller’s written consent.

**10 Indemnity**

Each party agrees to indemnify the other and keep indemnified the other against all claims and proceedings and all liability, loss, fines, costs and expenses incurred in connection therewith by either party as a result of:

10.1 Any claim made or brought by an individual or other legal person in respect of any loss, damage or distress caused to that individual or other legal person; and/or

10.2 Any claim or enforcement proceedings brought against either party as a result of the processing, unlawful processing, unauthorised disclosure or accidental loss of any personal data processed by either party, its employees, subcontractors or agents in either parties performance of the agreement or as otherwise agreed between the parties.

11 Law

This agreement is governed by and will be interpreted in accordance with English law. In the event of a dispute between the parties, it is agreed that the English courts will have non-exclusive jurisdiction to hear the case.

1. Third party rights

The parties are entering into this arrangement for the benefit of the parties and the individuals whose personal data the Processor will process each of which will be entitled to enforce it. No other person will have any enforceable rights under this arrangement and the Contracts (Rights of Third Parties) Act 1999 will not apply.

1. Responsibilities of the parties

The respective parties responsibilities are detailed below:

13.1 **Processor Responsibilities**

The personal data will be processed by the Processor in a secure “safe haven” environment and appropriate controls will be utilised in line with the current and legal (see Appendix 2) requirements of NHS Information Governance and ISO27002.

13.2 SLMS IGSG will be the responsible party for ensuring the investigation of any information security breaches involving the operation of the IDHS.

13.3 SLMS IGSG will ensure the annual NHS IG Toolkit assessment is undertaken and that this remains with a “satisfactory”, level 2 status.

13.4 Ensure that appropriate training is provided to all relevant personnel in relation to Information Governance and using all reasonable endeavours that they comply with the legal obligations of this agreement.

13.5 Ensure with all reasonable endeavours that suitable and robust access control procedures are in place to enable only suitably authorised personnel have access on a need to know basis.

13.6 Appropriate audit controls must be in place and these must be secured from unauthorised access or modification.

13.7 Ensure with all reasonable endeavours that the incident management procedures are followed, that the other party is briefed and corrective action is taken to redress any failures within a reasonable period of time.

13.8 **Data Controller’s Responsibilities**

That all relevant staff are aware of this agreement’s legal obligations and their responsibilities in discharging their duties.

13.9 Ensure by all reasonable endeavours that a local procedure is in place to facilitate timely approval of requests for data sharing in respect of this agreement.

13.10 Ensure that appropriate training is provided to all relevant personnel in relation to Information Governance and using all reasonable endeavours that they comply with the legal obligations of this agreement.

13.11 Ensure that the incident management procedures are followed, that the Processor is briefed without delay and any corrective action is taken to redress any failures within a reasonable period of time.

13.12 Ensure that standards and procedures are implemented to facilitate consent to disclose personal data constitutes informed consent and is given freely. A record should be kept of service users' consent given or withdrawn. The standards and procedures adopted should meet the practical measures required in the Information Commissioner’s Office (ICO) Data Sharing Code of Practice, Chapter 6 Fairness and Transparency. A copy of this agreement will be placed in the Library of Information Sharing Agreements that is maintained on the UCL web site

13.13 Adequate, accessible, efficient and effective procedures have been implemented to address complaints for unauthorised disclosures or use of personal data.

Sign the enclosed copy of this agreement to indicate your agreement to its terms and return to the Information Governance Officer (contact details below).

Signed for and on behalf of the Signed for and on behalf of the Processor:

Data Controller

Signature: ...................................................... Signature: ……………………………………

1. (authorised signatory) (authorised signatory)

Print name: ..................................................... Print name: …………………………………..

Position: ………………………………………… Position: ……………………………………..

Date: ............................................................…. Date: ………………………………………..

UCL SLMS Operational Contact: [Information Governance Officer]:[A N Other] *[AN.Other@ucl.ac.uk]]* [(020) 3549 5120]

**Data Controller’s Operational Contact: [Role of relevant officer]:[A N Other]** [AN.Other@xxxx.xx.uk]] [(000) 0000 0000]

Appendix 1

|  |  |
| --- | --- |
| **Term** | **Description** |
| **Healthcare Medical Purpose (aka “primary uses”)** | Includes; the uses which directly contribute to the diagnosis, care and treatment of an individual and the Audit/Assurance of the quality of healthcare provided. **In these cases person identifiable data can be used, but only the minimum amount of data should be used, and appropriate safeguards should be in place.** |
| **Non-Healthcare Medical Purpose (aka “secondary uses”)** | Includes; the Management of Health Care Services, Preventative medicine, medical research, financial audit and the management of health [and social] care services. **In these cases generally “effectively anonymised” data should be used, unless consent has been gained from the patient or there are special circumstances, such as an overriding public interest, or a route such as via Section 251 of the NHS Act 2006 or the Health Service (Control of Patient Information) Regulations 2002. However, current constraints on data quality reduces the ability to carry out such activities using effectively anonymised data, with the consequence that central NHS policy objectives cannot be realised. In the interim period therefore, where data and business processes are being refined in order to enable the use of effectively anonymised data, it may be necessary to use person identifiable data temporarily. However the amount of person identifiable data used should be minimised, and appropriate safeguards should be in place.** |

**Appendix 2**

Relevant legislation and other standards for information sharing:

* Data Protection Act 1998
* Human Rights Act 1998
* Common law duty of confidentiality
* Freedom of Information Act 2000
* Access to Health Records Act 1990
* Caldicott Guardian Manual 2010
* Confidentiality NHS Code of Practice 2003
* Confidentiality NHS Code of Practice – Supplementary Guidance: Public Interest Disclosures 2010
* NHS Act 2006 (Section 251)
* NHS Information Governance Toolkit
* The Health Service (Control of Patient Information) Regulations 2002
* AIDS (Control) Act 1987; NHS (Venereal Diseases) Regulations 1974; NHS Act 1977, NHS Trusts and Primary Care Trusts
* (Sexually Transmitted Diseases) Directions 2000. [Legislative amendments are necessary to reflect organisational change.]
* Human Fertilisation and Embryology Act 1990: ss 31 & 33;
* Human Fertilisation and Embryology (Disclosure of Information) Act 1992.
* Information Commissioners Data Sharing Code of Practice (See Appendix 3 for checklist)

Appendix 3 – Information Commissioner’s Data Sharing Guide

|  |  |  |
| --- | --- | --- |
| **Checklist** | **Identified** | **Evidence and location** |
|  |  |  |
| Objective of data sharing | YES/NO |  |
| Data Protection Notifications exchanged between the parties | YES/NO |  |
| Privacy Impact Assessment or risk assessment conducted. | YES/NO |  |
| Potential benefits and risks for society of sharing and not sharing | YES/NO |  |
| Minimum necessary dataset used | YES/NO |  |
| Is the use of personal data necessary | YES/NO |  |

Appendix 4 – Definitions

|  |  |
| --- | --- |
| **Term** | **Explanation** |
|  |  |
| **AES 256 bit encryption** | Advanced Encryption Standard 256 bit encryption has been made mandatory for healthcare related data by the NHS. |
| **Anonymisation** | does not enable the linking of data to the same subject across several data records, or information systems. Consequently it is impossible to re-identify anonymised data. (source ISO/TS 25237:2008) |
| **Data Controllers in Common** | In relation to data controllers, the term jointly is used where two or more persons (usually organisations) act together to decide the purpose and manner of any data processing. The term in common applies where two or more persons share a pool of personal data that they process independently of each other |
| **Data Controller** | a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed. (source Data Protection Act 1998) |
| **Data Processor** | in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller (source Data Protection Act 1998) |
| **European Economic Area** | Consists of the following countries:  Austria; Belgium;Bulgaria;Cyprus; Czech Republic; Denmark; Estonia; Finland;  France; Germany; Greece; Hungary; Iceland  Republic of Ireland; Italy; Latvia  Liechtenstein; Lithuania; Luxembourg  Malta; The Netherlands; Norway  Poland; Portugal; Romania; Slovakia  Slovenia; Spain; Sweden; UK |
| **IDHS** | Identifiable Data Handling Service – a secure safe haven service provided by UCL SLMS. |
| **IGSG** | Information Governance Steering Group: UCL SLMS body responsible for the management of information governance. |
| **ISO27002** | The International Code of Practice for Information Security Management, detailing effective management controls to control information assets. |
| **Pseudonymisation** | is a method to link pseudonymised data to the same data subject across several data records, or information systems without revealing the data subject’s identity. Pseudonymisation can be either reversible or irreversible. (source ISO/TS 25237:2008) |
| **Personal Data** | means data which relate to a living individual who can be identified—   1. from those data, or   (b)from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual. (source Data Protection Act 1998) |
| **Publication Scheme** | Under the Freedom of Information Act, public authorities are legally obliged to publish and maintain a publication scheme. A publication scheme communicates to the public the various materials available and any associated costs. |
| **Safe haven** | either a secure physical location or the agreed set of administrative arrangements that are in place within the organisation to ensure confidential personal information is communicated safely and securely. (source NHS Connecting for Health) |
| **SLMS** | School of Life & Medical Sciences |
| **Subject access requests** | Requests in writing to a data controller requesting a copy of the personal data held about the individual making the request, or for a person for whom, they have the requisite legal power of representation. |
| **UCL** | University College London |
| **UCLP** | University College London Partners |