LONDON'S GLOBAL UNIVERSITY

SLMS Data Handling Guidance

1. Document Information	
Document Name	SLMS-IG04a SLMS Data Handling Guidance
Author	Trevor Peacock
Issue Date	29/03/2017
Approved By	Chair of SLMS IGSG
Next review	Three years

2. Document History		
Version	**Date**	**Summary of change**
0.1	14/02/2013	First draft for discussion
0.2	06/03/2013	Second draft revisions from Daniel Heather/Shane Murphy
0.3	08/03/2013	Alice Garrett minor revision and circulation to User Group
0.4	14/03/2013	Shane Murphy incorporated revisions from Anthony Peacock
0.5	19/03/2013	Shane Murphy incorporated revisions from Dr Declan Chard
1.0	13/08/2013	Approved by the Chair of IGSG
1.1	21/01/2014	Trevor Peacock added clauses forbidding use of user-owned devices
2.0	05/02/2014	Approved by the Chair of IGSG
2.1	15/04/2014	Trevor Peacock: addition of section 5.4
3.0	06/05/2014	Approved by the Chair of IGSG
3.1	22/03/2017	Half-hearted and failed attempt to update and remove policy elements: T.Peacock
3.2	28/03/2017	Complete re-write to focus on guidance: T. Peacock
4.0	29/03/2017	Approved by the Chair of IGSG

Introduction
Information is central to the world leading medical research undertaken at University College London School of Life and Medical Sciences (SLMS)

Research projects within SLMS frequently receive data from the NHS and other third parties and are required to provide assurance that data are properly managed in compliance with legal, regulatory and contractual requirements

It is therefore important to ensure that information is managed securely, and that appropriate data handling techniques are used to secure personal data and sensitive personal data processed by SLMS

This Guidance aims to set out responsibilities and key considerations for all researchers working with sensitive personal data. Further details of services to support the guidance can be found in Appendix A

Scope of this guidance

- Personal data and sensitive personal data regardless of format, e.g. electronic / manual / paper records.
- All research handling sensitive personal data within the SLMS
- All information systems purchased, developed and managed by, or on behalf of, SLMS
- Data handled by any individual directly employed or working on behalf of SLMS

This Guidance is in addition to the SLMS IG Policy, UCL Information Security Policy and Data Protection Policy

Principal Investigators
The Principal Investigator (PI), as Information Asset Owner (IAO) is accountable to the Senior Information Risk Owner (SIRO) and must ensure that their research team complies with:

- Legal requirements
- Regulatory requirements (such as the IG Toolkit)
- The terms of any contracts covering data (such as Data Sharing Agreements)

Delegation
The PI may delegate responsibility to an Information Asset Administrator (IAA) who becomes **responsible** for managing information and access within the study. However, the IAO remains **accountable** for proper information handling

Legal requirements – The Data Protection Act
The Data Protection Act 1998 sets out the legal requirements for processing personal data. All research using personal data must address the eight principles.

Note that within the Data Protection Act, the term **processing** refers to any activity involving the data and **subject** refers to the person to whom the data relates

Principle 1. Processed fairly and lawfully
Ensure that you have informed consent or Section 251 exemption as the lawful basis for processing the data. Fairness relates to using data as would be expected from the purposes you set out in the consent or section 251 application

2. Processed for limited purposes
Be clear from the outset about why you are collecting the data and what you intend to do with it. This should be reflected in the consent or Section 251 exemption. For existing research datasets, there's an exemption for research that allows further use as long as:

- It doesn't result in decisions affecting particular individuals
- It doesn't cause damage or distress to a particular individual

Principle 3. Adequate, relevant and not excessive
Identify the minimum amount of personal data required and don't hold more data than is needed. Take particular care if sending data to 3rd parties and consider how much, if any identifiable data needs to be transferred

Principle 4. Accurate and, where necessary, kept up to date
This is more of a concern for longitudinal studies, but in all cases, consider if you need to keep the data up-to-date and if so, ensure that you have mechanisms in place to do this in a robust and accountable way

Principle 5. Not be kept for longer than is necessary
Take into account funders requirements and expiry dates for data covered by contracts. Ensure that data is securely destroyed in line with UCL policy or contractual obligations. There's an exemption on extended retention for research, providing:

- It doesn't result in decisions affecting particular individuals
- It doesn't cause damage or distress to a particular individual

Principle 6. In accordance with the rights of data subjects
Data subjects have the right to withdraw consent, so you need to ensure that your study has facilities in place to manage this properly. Subjects have the right to prevent processing of their data, but only if it causes unwarranted and substantial damage or distress. In other cases you must only explain to the individual why you do not have to do so

Principle 7. Technical and organisational measures
Make sure you have adequate physical and technical security in place that prevents unauthorised access to the data. Ensure that all members of your research team have a clear understanding of policies and procedures and keep their IG training up-to-date. Be ready to respond to any breach of security swiftly and effectively.

Principle 8. Not transferred to other countries without adequate protection
Countries within the EEA are considered to have adequate data protection legislation
The ICO maintains a list of countries with adequate data protection legislation
Any transfers of data to the US should be covered by Privacy Shield
Model contractual clauses should be used if necessary

For advice on data protection, contact the UCL Data Protection Office

Regulation – the NHS IG Toolkit and other frameworks
The IG Toolkit is required for any data obtained from NHS Digital, including ONS mortality and cancer registry data. The toolkit provides a set of requirements that must be met by the study. The IG Advisory Service maintains an IG Toolkit for the SLMS.

Section 251 applications to the Confidentiality Advisory Group (CAG) require an IG Toolkit.

Other sources of data, such as the Department for Education's National Pupil Database set out specific requirements to be met, which cover processes, training and technical measures.

The IG Advisory Service provides support in meeting the above and other regulatory frameworks

Contracts: sending data to third parties
When sending data to a third party, you will need to issue a UCL data processing contract that the other party signs. The UCL Data Protection Office maintains a template data processing contract that can be used in these circumstances

Any data obtained under an IG Toolkit and passed to a third party needs to include references to the SLMS IG policy along with clear and enforceable statement of obligations, expectations and references to the procedures for confidentiality and security

If sending data that has been supplied to you under contract to a third party, please ensure that you comply with any restrictions included in the original contract relating to onward sharing

Contracts: data supplied to the study
Research studies often obtain data from national datasets under licence. Close attention must be paid to the associated contracts, which often include restrictions and stipulations on sharing, who can access the data and expiry dates, after which the data must be securely destroyed

All Data Sharing Agreements from NHS Digital require compliance with the UCL Data Sharing Framework Contract (DSFC), an overarching contract covering all NHS Digital contracts

Secure technical environments and the 'safe haven' model
Security is an often mis-used term. In the context of sensitive personal research data, security needs to be supported by a combination of technology, processes and training. Standard Operating Procedures (SOPs) help to ensure that the team work to a consistent standard and SOPs for security should include a clear desk policy, locking screens when away from desks and managing visitors to the secure area.

You should aim to have documentation to hand, such as SOPs, training records and audits that demonstrate an appropriate level of security.

A **safe haven** is a secure working environment with controls in place to manage access and permissions. Within a safe haven, there are controls to manage data transfer in and out of the environment. Documented procedures are used to ensure that activities are attributable to individuals and can be audited.

The UCL Data Safe Haven meets these requirements and is free-to-use for UCL studies.

Transfers of data can present a high risk. The following aspects should be considered:

- Does the data need to be transferred at all?
- Is the minimum necessary set of data being transferred?
- How often are data transferred?
- How is the data in transit protected from accidental or deliberate disclosure?
- For transfers out of the EEA, are data protection laws adequate in the receiving country?

For electronic data, **encryption** is a standard way to protect it in transit and at rest. The 7Zip de-facto standard provides adequate encryption to AES256 standards, as required by the NHS. Care should be taken to select a 'difficult' password and to transfer this via separate channel to the encrypted data. It is also important to determine the security the environment

to which the data will be transferred, to address the risk of data being stored insecurely once received.

For paper records, secure couriers, tamper-evident envelopes and containers could be considered. In all cases, where appropriate, a SOP should be in place to confirm receipt, to provide assurance that the data has reached the correct destination.

The IG Advisory Service provides an **Information Risk Assessment Tool** to help assess the security of data transfers

Data destruction
Specific attention should be paid to destroying personal data. Robust authorisation procedures should be in place to avoid accidental destruction. Destruction should be undertaken in accordance with recognised standards and particular care should be taken at the end of a contract to ensure that third parties properly destroy any data shared with them.

Anonymisation, re-identification and pseudonymisation and onward sharing of data
Truly anonymised data cannot be traced back to an individual. It is rare for personal data to become truly anonymised because factors such as small sample sizes and rare attributes, when combined with other sources of data, can provide enough information for a 'jigsaw attack'.

Substituting pseudonyms for identifiers results in pseudonymised data, in which the pseudonym 'key', linked to the identifiers, is usually kept securely and separately to the payload data. This retains the ability to link back to the original individual, so this type of data is potentially personal. Consideration should be given to the need to retain a link to the individual and the likelihood of re-identification from the payload data. For the purposes of the Data Protection Act, pseudonymised data carries a risk of re-identification which should be assessed, taking into consideration the type of payload data and the context of any onward sharing

Where identifiable or potentially identifiable personal data is to be shared, this must be in accordance with the Data Protection act, which means there must be a legal basis and the consent must explain the purpose and context for the onward sharing. You must also take account of any contractual restrictions on onward sharing of data. Sharing of data outside of the EEA needs to satisfy principle 8 of the Data Protection Act. All sharing must be lawful and appropriate and respect NHS service user wishes

Joiners, movers and leavers
Within a study, access to sensitive data must be controlled. Those authorised to work with the data must be granted access, understand the study's procedures for data handling and complete annual IG training. During the study, team members will leave or move to other parts of UCL, in which case, access to physical and electronic resources must be revoked. Records of should be kept as evidence that access to data is properly managed.

Appendix 1: Additional resources

Data Protection Office
http://www.ucl.ac.uk/legal-services/dp-overview

Onward sharing of data
https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf
See chapter 7: Different forms of disclosure (p36)

NHS Digital Data Sharing Framework Contract for UCL
http://www.ucl.ac.uk/isd/itforslms/services/handling-sens-data/approved-documents
(First document in the list)

IG Advisory Service
http://www.ucl.ac.uk/isd/itforslms/services/handling-sens-data/info-gov-advisory

UCL Data Safe Haven
http://www.ucl.ac.uk/isd/itforslms/services/handling-sens-data/tech-soln

Information Risk Assessment Tool
http://www.ucl.ac.uk/isd/itforslms/services/handling-sens-data/approved-documents
(See SLMS-IG-11a in the Templates and Tools section)

Joiners and Leavers template checklist
https://www.ucl.ac.uk/isd/itforslms/services/handling-sens-data/Joiners-movers-leavers/

Anonymisation guidance
https://www.ucl.ac.uk/isd/itforslms/services/handling-sens-data/anonymisation/

Delegation of responsibility to an IAA by an IAO
(TBC)

Encryption guidance
https://www.ucl.ac.uk/informationsecurity/itsecurity/knowledgebase/securitybaselines/encryption