Principal Investigator Obligations

All research and researchers have a duty of care to comply with legal requirements and with UCL and SLMS policies, procedures and guidelines.

Personal or sensitive personal data must be fairly obtained with all appropriate informed consents.

Transfers of personal or sensitive data outside of the European Economic Area (EEA) must be registered with the UCL Data Protection Officer, Legal Services. The territory should have data protection regulations equivalent to the UK in place. Failing this a contractual arrangement is required that specifies appropriate information governance obligations for the third party.

Personal data can also be securely protected using encryption, pseudonymisation and anonymisation techniques.

Data Protection Act

Researchers should be aware that they must comply with the eight principles of the Data Protection Act 1998. The 7th principle requires appropriate information security to be in place. A contravention of the data protection principles can result in a penalty of up to £500,000.

If you lose personal or sensitive personal data you can face a fine of up to £500,000 from the Information Commissioner’s Office (ICO).

Caution Matching Datasets

If matching with other datasets, take care that importing rare medical conditions, ethnicity and postcode data can potentially make it personal sensitive data and that the security controls are appropriate. There may be a need to encrypt or de-identify the data.
Purpose of this guide

This guide has been put together to assist research study Principal Investigators (PIs) handling identifiable data.

Within the School of Life and Medical Sciences (SLMS) PIs frequently handle large volumes of data received from external organisations much of it of a sensitive nature. We need to ensure that the data is handled in a way that complies with the standards of the information providers and respects the interests and preferences of the research subject.

Some definitions...

**Personal data** is any information that can identify an individual.

**Sensitive data** is personal data that can be one or more of the following: mental or physical health; sexual life; ethnicity; religious or other similar beliefs; trade union membership; political opinions; criminal offences or potential offences committed and any associated sentence.

---

**Working with NHS data**

Identifiable data from NHS patients can be used in clinical research if consent has been obtained with clarity regarding its use, if the organisations which will have access have been identified and if patients are informed that their data will be transferred outside the UK. If not the study must apply to the Health Research Authority (HRA) for a S251 exemption. Otherwise the Information Commissioner could impose a fine of up to £500,000.

S251 exemption now requires compliance with the NHS IG Toolkit at Level 2 or above. The NHS IG Toolkit is a set of standards for measuring information governance, within UCL compliance is typically requested by research study teams under the ‘Secondary Hosted Use Team/Project’ category which measures compliance with 14 standards.

Further guidance on gaining NHS IG Toolkit accreditation can be found at:

www.ucl.ac.uk/slms/ident-data/

---

**Securing Personal and Sensitive Data**

Personal data should be processed in the EEA, if this isn’t possible sufficient measures should be put in place, if in doubt check with the Data Protection Office.

Approved mechanisms for transferring this type of data include:

- AES 256-bit encryption or higher of email attachments using a tool such as 7-Zip or WinZip
- NHSmail is secure when both the sender and receiver have a NHSmail address (with the suffix @nhs.net)
- Public key encryption of emails using a tool such as OpenPGP using AES 256-bit encryption or higher encryption
- The IDHS system will be providing a secure FTP web portal which can be accessed outside of the UCL network
- Report all information incidents to the Computer Security Team http://www.ucl.ac.uk/cert/reporting.html

For further advice and guidance:

www.ucl.ac.uk/slms/ident-data/

---

**Contact**

Email: slms.pid@ucl.ac.uk
Web: www.ucl.ac.uk/slms/ident-data/

---

**Don’t...**

- ignore the Data Protection Act’s eight principles
- disclose personal data without confirming the identity of the recipient and that they have a justifiable need to know
- send any more personal data than the minimum necessary dataset
- where an alternative is available, send personal or sensitive personal data by fax
- access websites that may contain inappropriate or offensive material
- include personal or sensitive data in the title of your email message
- download files or open email attachments without being absolutely certain that you can trust the sender and the content
- send or forward junk mail, chain letters or virus warnings – these may be hoaxes or dangerous.