SGUL Data Handling Guidance for Principal Investigators

1. **Document Information**	
Document Name	SGUL Data Handling Guidance for Principal Investigators
Author	
Issue Date	
Approved By	Chair of SGUL IGSG
Next review	

2. **Document History**		
Version	**Date**	**Summary of change**
0.1	17/02/2016	First draft for discussion
1.0	18/02/2016	SIRO final approved version
2.0	04/12/2018	IGSG Approved

Table of Contents

Introduction **3**
Scope of Guidance **3**
Obligations for all Principal Investigators **3**
Data Protection Act 2018 implications for Research **4**
Securing personal and sensitive personal data **6**
Appendix 1: The Data Protection Principles **8**
Appendix 2: Definitions **9**

1.0 Introduction

1.1 Information is a vital asset, both in terms of the world leading clinical research undertaken at St George's, University of London(SGUL) and the efficient management of services and resources.

1.2 Research projects within SGUL frequently receive data from NHS partners and other third parties, as a result SGUL is subject to NHS Information Governance responsibilities in satisfying the NHS and other information governance requirements required by third parties or SGUL Partners.

1.3 It is therefore of paramount importance 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 SGUL.

1.4 This Guidance will define the data considered to be personal and sensitive personal data and the approved methods for securing these data.

2.0 Scope of Guidance

2.1 The scope of this guidance applies to personal data and sensitive personal data regardless of format, e.g. manual/paper records generated at SGUL as well as electronic data.

2.2 All research and researchers have a duty of care to comply with all legal requirements and with SGUL policies, procedures and guidelines

2.3 Data defined as personal or sensitive personal data must be encrypted using 256 bit AES Encryption.

2.4 Personal data can also be securely protected using pseudonymisation or anonymisation techniques.

2.5 This guidance covers all information systems purchased, developed and managed by, or on behalf of, SGUL and any individual directly employed or otherwise by SGUL.

2.6 This Guidance is in addition to the SGUL Data Protection Policy and applies to all staff and students of SGUL and all other computer, network or information users authorized by SGUL or any department thereof. It relates to their use of any SGUL-owned facilities (and those leased by or rented or on loan to SGUL), centrally managed or otherwise; to all private systems (whether owned, leased, rented or on loan) when connected to the SGUL network; to all SGUL-owned or licensed data and programs (wherever stored); and to all data and programs provided to SGUL by sponsors or external agencies (wherever stored).

3.0 Obligations for all Principal Investigators

3.1 Principal Investigators (PIs) must ensure that processing of personal or sensitive personal data occurs when there is a clear purpose for doing so.

3.2 PIs must ensure that personal or sensitive personal data has been fairly obtained and where necessary all suitable informed consents have been obtained for the purpose and intended use such as disclosure of sensitive personal data. PIs must ensure observance and compliance with the Data Protection Act 2018.

3.3 Confidentiality is of paramount importance in the use of personal or sensitive personal data and the privacy of individuals comes first. PIs and their staff shall ensure they are familiar with the requirements of the NHS Code of Practice on Confidentiality.

3.4 PIs must ensure they have mechanisms in place to uphold the right of individuals to withdraw their consent for processing.

3.5 PIs must ensure that all personal and sensitive personal data is suitably secured as outlined in sections 3.2 and 3.3 of this Guidance, at all times.

4.0 Data Protection Act 2018 implications for Research

4.1 There are exemptions under the DPA relating to research purposes. The exemptions are only applicable where the data is not processed to support decisions in respect of individuals. The exemptions can only be exercised when the activity is not detrimental to the legitimate rights of individuals and will not cause damage nor distress.

4.2 Researchers should be aware that they must comply with the Data Protection Act 2018 and this is also a requirement of the S251 process detailed below. A contravention of the Data Protection Act can result in a penalty of up to £17M. Transgression of the Data Protection Act will result in the SGUL considering disciplinary action against researchers.

4.3 The purposes for processing of personal and sensitive personal data for research are not always determined or known at the point of obtaining the data. Typically researchers will use information that has already been collected by others. The DPA requires that the data is obtained fairly and lawfully. In English law this means that the individuals must be provided with informed consent, understanding for what purpose(s) the data will be used and understanding the disclosures of personal data and any overseas transfers that will be made. Research therefore must be indicated as a purpose at the point of collection when routine health care is provided, or when individuals are subsequently approached to consent to their data being used in clinical research. Failure to do this will mean a potential breach of the DPA.

4.4 The new DPA 2018 legislation was written with research in mind, in fact one of the additional conditions for holding and using special categories of personal data (for all organisations, public authority or otherwise) is: (Article 9):

- processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for

suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

4.5 The circumstances in which the exemption is applicable requires:

- That further processing is not incompatible to the purpose for which the data was obtained;
- Personal data for research purposes may be kept indefinitely; and
- The right for individuals to obtain copies of their personal data is waived provided that the research results do not identify individuals.

4.6 The use of personal and sensitive personal data for research purposes without consent is regulated under Section 251 of the NHS Act 2006. Responsibility for regulating the application of Section 251 has been migrated to the Health Research Authority (HRA) from the National Information Governance Board (NIGB) as of 31st March 2013. Researchers need to approach the Confidentiality Advisory Group (CAG) and submit applications. Each application is considered and the Secretary of State approves the application on the advice of the CAG. The CAG will assess if there is sufficient justification to process the personal data and may put forward recommendation for additional conditions to be complied with. The process establishes a legal basis to disclose personal or sensitive personal data without being in breach of the common law duty of confidentiality.

4.7 Researchers should make themselves familiar with the S251 approval process. Further information and guidance is available at the CAG Application Process, and in particular the pre-application decision tool. One of the key questions is concerned with whether consent can be reasonably sought from individuals. CAG will need to be convinced that obtaining consent from individuals would involve disproportionate effort. To make use of this exemption, researchers will need to document the reasons why disproportionate effort to gain consent would be required. This assessment should include relevant factors e.g. cost, time and ease of provision of information to the individual (if the data was collected in the past it may be impossible to contact the individuals) weighed against benefits to the individual.

4.8 The purpose for the research must establish a genuine public interest and/ or show that the research is capable of delivering improved patient care.

4.9 Researchers must also provide a cogent argument that the use of pseudonymised or anonymised data cannot be used to progress the research. Evidence must be provided to show that the research cannot progress with de-identified data due to cost and available technologies.

4.10 Researchers must respect the rights of individuals for them to withdraw consent for the processing of personal data or sensitive personal data.

4.11 Any transfers of personal or sensitive personal data outside of the European Economic Area (EEA) must be registered under the DPA

with the SGUL Data Protection Officer, IT Services. It is essential that before such transfers take place the territory has in place adequate data protection regulations that are broadly similar to the UK DPA 2018. A contractual arrangement should be in place that specifies appropriate information governance obligations for the third party. Researchers must be cautious when considering overseas transfers and seek specialist advice from the SGUL Data Protection Officer prior to progressing such transfers.

4.12 The use of personal data for research is exempt from the requirement to keep personal data current. However, this is on the proviso that the following conditions are met:

- Individuals privacy and identity are respected
- The data is not used to make decisions in respect of individuals
- Legitimate interests of individuals are respected to prevent possible damage or distress.

5.0 Securing personal and sensitive personal data

5.1 This type of data must never be held on systems external to the SGUL with the exception of secure environments provided by trusted SGUL partners. For the avoidance of doubt this type of data must never be held on personal email accounts. If in any doubt please contact the SGUL Data Protection Officer. Transgression of this clause 5.1 will result in disciplinary action being taken by SGUL. SGUL email is not a secure environment for the processing of personal and sensitive personal data unless you use one of the appropriate approved mechanisms in 5.3 below.

5.2 The SGUL requires that all personal data is processed in accordance with the Data Protection Act 2018 and where possible all person identifiable and sensitive personal data must be processed within EEA. If this is not possible then suitable safeguards to protect the privacy rights of individuals must be assessed. If legislation in the country of processing is not broadly equivalent to the UK Data Protection Act 2018 then contractual arrangements should be in place to provide the requisite level of protection.

5.3 The approved mechanisms for protecting this type of data for SGUL includes the following:

- Secure folder set up by IT Services within a on a secure central server – this provides a data safe haven (DaSH) environment in which personal data and sensitive personal data can be processed. Access to the folder is controlled under the authority of the researcher who originally created the folder.
- IT Services instruction on use of 7Zip to securely transfer personal and sensitive personal data – instruction on how to securely transfer files containing sensitive personal data (e.g. personal identifiable data (PID)).
- NHS Mail Service – Patient identifiable data can be transmitted securely when you use nhs.net to nhs.net email transfer.

- SGUL Pseudonymisation rules - If you use identifiable patient information for your research, you should use anonymised or pseudonymised data wherever possible.

Appendix 1: Definitions

Personal Data:

a) Information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier such as:
    - name,
    - an identification number,
    - location data,
    - an online identifier
b) or to one or more factors specific to the:
    - physical,
    - physiological,
    - genetic,
    - mental,
    - economic,
    - cultural or
    - social identity;

Processing - covers any activity from obtaining the personal or sensitive personal data through its lifecycle to destruction. This includes but is not limited to the following: printing; viewing; transferring; performing analysis; amendment; erasure and destruction.

Special Category Data – is personal data consisting of information as to:

- race;
- ethnic origin;
- politics;
- religion;
- membership of a trade union;
- health;
- sex life;
- sexual orientation;
- genetics;
- biometrics (where used for ID purposes)