1. Introduction

1.1 This is a guidance note for those wishing to enter into a Data Sharing Agreement with the Health and Social Care Information Centre (HSCIC). The data provided by HSCIC is often of a highly sensitive nature and it is therefore important that there is strict adherence to the data security requirements set out in the University’s Information Security Policy and those specified by HSCIC. The purpose of this document is to provide specific guidance on the requirements set by HSCIC which complement those of the University.

1.2 The HSCIC is the national provider of information relating to health and from whom the University obtains data for research purposes. In order to obtain data from HSCIC the University has entered into a Data Sharing Framework Contract at an institutional level with HCSIC.

1.3 In addition to the above, for each request for information there needs to be in place a Data Sharing Agreement (DSA) signed by the person requesting the information.

1.4 In processing the data obtained, the requestor (referred to subsequently as the Data Recipient) must comply with the provisions of both the Framework Contract and the DSA.

1.5 Failure to comply with the provisions of the Framework Contract and DSA may not only affect individual projects but could result in termination of the Framework Agreement and the entire University being denied access to data from HSCIC.

2. Framework Contract

2.1 The Framework Contract may be accessed using the following link: (Link to be added)

2.2 The University has clearly entered into the contract on the understanding that the contractual obligations can be met. However, it must not be assumed that these requirements are automatically met. Specific action will be necessary to ensure compliance. They must be also considered in the context of each DSA.

2.3 Data Recipients must read the Framework Contract in conjunction with the DSA. Data Recipients need to be aware of and adhere to the specific undertakings given in the Framework Contract which will be applicable if not otherwise over-ridden in the DSA.
2.4 **Staff wishing to enter into a DSA should consult with either their College IT or IT Services to ensure that their proposed processing of the data meets contractual obligations.**

2.5 This guidance note is primarily concerned with meeting obligations with respect to the data. Before entering into a DSA, staff should also check that other provisions within both the Framework Agreement and the DSA are acceptable.

2.6 **In signing the Framework Contract the Registrar has given an undertaking that the University will comply with the requirements of the Framework Contract. In order to be able to demonstrate compliance, if the DSA does not explicitly state a requirement to comply with the requirements of the Framework Contract it will be necessary to provide the Registrar with written assurance of adherence to the specific obligations within the Framework Agreement and the DSA.**

2.7 If clarification is required on any points, this may be obtained by contacting Information Assurance Services (IAS).

3. **Contractual Data Requirements**

3.1 Data Recipients must meet the requirements as set out in the Framework Agreement. In particular, attention is drawn to the following:

a) **Part 2 – Section 3 Licence and IPR including**
   - Prohibition on sub-licensing the data without the consent of HSCIC
   - Intellectual Property Rights *(See Section 6 below)*
   - Copyright notice obligations
   - Compliance with HSCIC, NHS and ONS standards where appropriate

b) **Part 2 - Section 4 Data Recipient Responsibilities including**
   - Designation as Data Controller for personal data
   - Purpose for processing limited to that stated in the DSA
   - Prohibition on third-party access and sharing of data without the consent of HSCIC
   - Staff training requirements
   - Destruction of data requirements
   - Notification of breaches to HSCIC *(through IAS)*
   - Notification of requests for access to HSCIC *(through IAS)*
   - No combination with other data or identification of individuals without the consent of HSCIC
   - Compliance with data security requirements *(see below)*
   - Undertaking of a risk assessment prior to publication

c) **Part 2 - Section 5 Data Protection including**
   - Compliance with the Data Protection Act
   - Maintenance of good information governance standards equal to relevant NHS Information Governance Toolkit Standards *(see below)*
- Prohibition on transfer outside of the EEA without the consent of HSCIC
  (Note that this may prohibit the use of Cloud-based services)
- No publication of the data without the consent of HSCIC
- No dissemination of the data without the consent of HSCIC
- Reliability of staff
- Access to data restricted to only those staff with a need to access
- No contact with data subjects without the consent of HSCIC
- Sub-contracting processing of the data not permitted without the consent of HSCIC

d) Part 2 - Section 6 Confidentiality
e) Schedule 2: Data Security Requirements (see Sections 4 and 5 below)
f) Schedule 3: List of relevant legislation and standards

3.2 HSCIC may require information, assistance and co-operation to establish the University’s compliance with the agreements. It should be noted that HSCIC have the right to conduct an audit to ensure that contractual obligations are being met, and to make a charge for such audit where evidence of non-compliance is found.

4. Data Security Requirements

4.1 HSCIC require that the data (including both personal and non-personal data) will be processed in compliance with either the requirements of the NHS Information Governance Toolkit or the Information Security Standard ISO 27001, or that good information governance practices are maintained.

4.2 The University is currently not accredited to these standards. It has therefore been indicated that other assurance is in place i.e. the University’s Information Security Policy which is based upon the ISO 27001 standard.

4.3 Whilst the University’s Information Security Policy does not meet either of the specified standards, it does stipulate good information governance practices. Compliance with the University’s Information Security Policy, in conjunction with meeting the specific standards set out in the Framework Contract should provide a level of assurance acceptable to HSCIC.

4.4 However, for personal data, this may not always be the case. The Data Sharing Agreement requires that the Data Recipient shall ‘maintain good information governance standards and practices, meeting or exceeding the IG Toolkit standards requires of its organisation type’.

Note: Advice should be sought from either IT Services or College IT.

5. Key Data Security Concerns

5.1 The Framework Contract and the DSAs set out a number of obligations, chief of which is to provide a level of security appropriate to the nature of the information and the state of technological development. It should be noted that the requirements apply to both personal and non-personal data.
5.2 The key requirements are detailed below.

a) Access to the data must be restricted to only those staff who have a need to access the data.

b) All staff must be properly trained in data protection prior to their use of the data and such training is to be repeated at regular intervals. There should also be evidence that they have understood the training.

Note: To meet this standard it would be acceptable for staff to have undertaken NHS data protection training and assessments, and completed NHS refresher training on an annual basis. This would be additional to completion of the University’s Information Security Awareness training. In 2015, the Information Security Awareness Training will include assessments and a refresher module.

c) There is a requirement for vetting of staff both during recruitment and throughout their engagement in the processing of the data, and for processes to be in place for identifying changes in personal circumstances which may have a bearing on compliance.

Note: Guidance on meeting this requirement should be sought from the College and Human Resources.

d) IAS must be informed of any risk to the data which becomes apparent, who will in turn inform HSCIC as appropriate.

e) Access rights must be properly configured and well-defined joiners and leavers processes in place.

f) Controls in place to make sure that complex alphanumeric passwords are required for access to the data and that training is provided in relation to the need to keep such passwords secure;

g) Procedures in place to identify wrongful use of data, including the monitoring of wrongful access to data;

h) Suitable and effective authentication processes must be established and used to protect data.

Note: The requirement will vary dependent on the nature of the data. Guidance should be sought from College Computing and/or IT Services.

i) Data must be backed up on a regular basis and all back up data subject to such security procedures as are necessary in order to protect data integrity, such security measures being commensurate to the nature of the data.

j) All backup data and other personal information must be transported in a safe and secure manner;

k) All electronic data in transit must be encrypted.
l) All data held on portable media must be encrypted. This applies to all portable media including mobile phones, tablets, laptops, external disk drives and USB datasticks.

m) A register of all assets containing personal data, and including portable media, must be maintained and details of disposal recorded.

n) The data must not be accessed off-site or via a privately-owned electronic device other than through a secure electronic network.

o) Data must not be stored on privately-owned devices irrespective of whether the device is encrypted.

Note: As the University does not currently offer a service for secure off-site access, remote processing of the data is not permitted, as is the use of privately-owned devices.

p) All data must be disposed of in accordance with the guidance given in the University’s Records Management Policy and a record of destruction maintained.

q) Compliance with the above and the University’s Information Security Policy to be audited on a regular basis and at least annually.

5.3 Please note that consideration of the above is not a substitute for consideration being given to both the Framework Contract and DSA.

6. Additional Undertakings

6.1 As the University cannot demonstrate compliance with the NHS Information Governance Toolkit or the Information Security Standard ISO 27001 the Framework Agreement requires the following undertakings to be given:

a) Process Personal Data only for the provision of health care or adult social care, or the promotion of health, and only for purposes described in this Contract and the relevant DSA, and which are consistent with the purposes recorded in the Data Recipient’s data protection registration with the Information Commissioner’s Office.

b) Request and process the minimum data necessary (e.g. using age range rather than age if sufficient).

c) Deploy secure processes, procedures, practice and technology for storage and access, commensurate with the Personal Data being processed.

d) Ensure the rights of individuals are met, such as satisfying subject access requests received, ensuring data accuracy and correcting errors, and handling objections and complaints.

e) Permanently destroy/delete or erase the Data once it is no longer required for the purpose for which it was collected and confirm destruction to the HSCIC;
f) Ensure all Personnel with access to Personal Data provide a written undertaking that they understand and will act in accordance with the DPA, will not share passwords, and will protect the confidentiality of the Personal Data.

g) Report immediately to the HSCIC any security incidents relating to the Data, and any instances of breach of any of the terms of this Contract.

h) Comply with any specific legislation in relation to the Data (such as the Statistics and Registration Services Act 2007).

6.2 Of the above, c), d), e) and g) will have been addressed in the earlier sections

7. Intellectual Property Rights

7.1 Clause 3.3 of the Framework Agreement gives HSCIC rights to Intellectual Property Rights in a derivative work. HSCIC have agreed that this was not intended. Whilst they are not prepared to change the Framework Agreement they have agreed that this clause may be qualified in the DSA.

7.2 IT IS THEREFORE ESSENTIAL THAT YOU INCORPORATE THE FOLLOWING CLAUSES INTO YOUR DSA:

   a) The Intellectual Property Rights in the Data shall remain at all times the property of the HSCIC. All rights in the Data not expressly granted under the relevant DSA are reserved to the HSCIC.

   b) The Intellectual Property Rights in Derived Data shall remain at all times the property of the Data Recipient. For the purposes of this clause, “Derived Data” means any data (wholly or in part) manipulated or added to, such that it: (a) cannot be identified as originating or deriving directly from the Data; and (b) is not capable of use substantially as a substitute for the Data.

   c) Clause 3.3 of the Data Sharing Framework Contract shall not apply to this DSA.

---

Failure to comply with University Policy may lead to disciplinary action.

The official version of this document will be maintained on-line. Before referring to any printed copies please ensure that they are up-to-date.