Introduction to Information Governance (IG) & the IG Toolkit

Content

1. What is Information Governance (IG)?

2. When and why might IG be an issue for me?

3. Information Governance - Why?

4. How the University can provide IG assurance

5. The College and IG / the IG Toolkit

6. How you use and provide evidence for the IG Toolkit?

7. What does this mean to me? – What do I have to do?
What is Information Governance (IG)?

Put simply Information Governance is to do with the way organisations ‘process’ or handle information – including standards, systems and processes.

It covers personal information, i.e. that relating to patients/service users and employees, and corporate information, e.g. financial and accounting records¹.

It is therefore relevant when handling - generating, accessing, sharing, analysing and otherwise using - health care information (whether defined for example, personal, sensitive, ‘person identifiable’, pseudonymised or anonymised).

Given the plethora of questions and definitions in this area (‘what is regarded as secure data’, ‘what does pseudonymised mean’, ‘am I a data controller or processor and what are the implications’ etc.) this document provides an introduction and doesn’t attempt to provide the answers to all detailed questions which come from the specifics of research activity.

In the context of research within CMBSP, IG can be seen to be a subset of research data management in general, and consisting of a broad range of concerns:

---

¹ https://www.igt.connectingforhealth.nhs.uk/about.aspx
² Image courtesy of Sussex Community NHS Trust
Research Data Management Advice and support can be found at the University RDM website – www.le.ac.uk/researchdata and via email at rdm@le.ac.uk:

The Breath of Information Governance

In the context of the University Information Governance is a broad concern encompassing:

a) **Information Governance Management** (responsibility for IG, University policy, training, responsibilities)

b) **Confidentiality and Data Protection Assurance** (link to Information Assurance Services, implementation of requirements, Information Security Policies)

c) **Information Security Assurance** (Information Security Management, risk management, information asset inventory and ownership, policy, incident management, maintenance of confidentiality, integrity and availability of data, anonymisation and pseudonymisation, secure data processing/secure data processing environment)

d) **The process of generating IG Toolkit** submissions which relies on, and in turn drives development in the areas above.
As a result IG concerns variously Colleges (researchers therein), Research Governance, IT Services (central and College based), Information Assurance Services, Library, Research Support Office, Lifelong Learning, EBD, and the relationship between these in order to create a comprehensive, coherent, co-ordinated and consistent approach.

The rest of the document is written on the basis that IG includes issues across the Research Data, Governance and Information Security domains e.g. a researcher states in their proposal that access to sensitive data are secure, that is questioned through Sponsorship, it relies on appropriate IT services being available, these comply with what is in University Information Security Policy, which reflect legislation and ISO standards.
What is “Personal Data”?

Personal data (according the Information Commissioner’s Office or ICO) means data which relate to a living individual who can be identified:

a) 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 (Ref. 1).

In practice this means:
Information about a person which would enable that person’s identity to be established by one means or another. This might be fairly explicit such as an unusual surname or isolated postcode or items of different information which if taken together could allow the person to be identified. All information that relates to an attribute of an individual should be considered as potentially capable of identifying them to a greater or lesser extent.

What is “Sensitive Personal Data”?

Sensitive personal data (according the ICO³ – Ref. 1) means personal data consisting of information as to:

a) the racial or ethnic origin of the data subject,
b) their political opinions,
c) their religious beliefs or other beliefs of a similar nature,
d) whether they are a member of a trade union,
e) their physical or mental health or condition,
f) their sexual life,
g) the commission or alleged commission by him of any offence, or
h) any proceedings for any offence committed or alleged to have been committed by him.

In practice this means:
Information, which if lost or compromised could affect individuals, organisations or the wider community. This is wider than, but includes, information defined as sensitive under the Data Protection Act 1998.

---

2. When and why might IG be an issue for me?

Case 1: Several months after completion of data analysis a Principal Investigator needs to access this work. They realise that it was held on a personal (\Z) data drive by a member of the team who has left the country.

*Is there any way that data can be recovered?*

*Has the user account and data been deleted?*

*Did they take sensitive data with them?*

Dealing with IG involves:

a) researchers facing challenges which relate to the data they are concerned with,

b) what exists at the University to deal with this (people, advice, processes, IT), and

c) the University providing an IG framework which needs to be applied in a practical context.

Proposal stage: IRAS forms, HSCIC DARS (Data Access Request Service) process, data sharing agreements, data management planning, funder requirements.

A38. How will you ensure the confidentiality of personal data? *Please provide a general statement of the policy and procedures for ensuring confidentiality, e.g. anonymisation or pseudonymisation of data.*

IRAS v4.0.0
Proposal Stage: The Research Governance and Sponsorship process e.g. questions on the Joint Office Risk Assessment form for Research Sponsorship

*Is identifiable data being stored outside of the NHS?*

*Do you plan to transfer data between different organisations? e.g. UoL and the NHS.*

During research: Who gets access, what IT infrastructure in place

*What is the method for secure transfer of data, to a secure network location, with daily data backup, and with appropriate controlled access to the research group?*

After completion: Organisations such as HSCIC may contact you to detail data destruction - where are all copies of data, where are backups? How do I know that data has been deleted from a PC? What is a certificate of destruction and how do I get one? Have HSCIC Data Destruction requirements been followed?

---

![HSCIC Logo](https://example.com/hscic_logo.png)

**CERTIFICATE OF DESTRUCTION**

The Data Sharing Agreement / Data Reuse Agreement you have with the HSCIC has expired.

In accordance with the terms of your agreement you are now requested to confirm that all data has been destroyed and this should include the original data plus any copies.

---

IG issues are therefore integral to the routine progress of research, and things to remember are:

a) They are important as they may relate to compliance with legislation

b) They may present significant challenges

c) Support exists to provide solutions

---

**Case 2:** As part of an application process for access to NHS patient data the organisation holding that data asks for evidence that the recipient organisation is registered with and has successfully submitted an IG Toolkit, and can demonstrate the IG Framework in place.

*Is the University or College or research group covered under the IG Toolkit and what evidence does that allow me to provide?*
3. Information Governance - Why?

In addition to the active expectation of compliance with applicable legislation a range of regulators, those providing data such as HSCIC, and research funders are taking a more robust and comprehensive approach to the management of data.

This demands the ability to a) maintain confidentiality, integrity and availability of data, through people (with appropriate skills and training), processes and framework of responsibility, and technical means, alongside b) the means to actively evidence that this is a reality.

Specific examples of challenges include new HSCIC institutional Framework Contracts (see below) and linked research level Data Sharing Agreements, requirement to complete IG Toolkit (including Section 251), EU Data Protection regulations (2015)\(^4\) which will lead to a new UK Data Protection Act, and (changes to) the MHRA inspection regime.

With the impact of Caldicott \(^5\) and the fall-out from Care.data\(^6\) there are increased concerns to provide assurance that sensitive data is shared and managed appropriately. This relies on evidence of correct practice.

Information Governance provides a way for people to deal consistently with the many different rules about how information is handled, including those set out in:

- The Data Protection Act 1998.
- The common law duty of confidentiality.
- The Confidentiality NHS Code of Practice.


• The NHS Care Record Guarantee for England.
• The Social Care Record Guarantee for England.
• The international information security standard: ISO/IEC 27002: 2013.
• The Information Security NHS Code of Practice.
• The Records Management NHS Code of Practice.
• The Freedom of Information Act 2000.

**Good IG provides assurance** - assurance to the public and organisations working with you, that information governance is taken seriously – there is good practice, appropriate processes, structures, systems, trained staff – and information is handled appropriately.

### 4. How the University can provide IG assurance

The University provides assurance generally through its implementation of:

- a) An IG Framework (defining responsibility etc.)
- b) Policies
- c) Processes e.g. Research Governance Sponsorship
- d) Services e.g. IT infrastructure
- e) Appropriately skilled staff who have undergone training
- f) Formal submission of evidence

Submission of evidence includes:

- a) Research proposals and Data Management Plans\(^7\) ([www.le.ac.uk/researchdata](http://www.le.ac.uk/researchdata))
- b) ISO27001 certification - increasingly it is questioned whether there is University certification under the Information Security Management standard (there is no current University certification)
- c) Information Governance Toolkit (IGT) submission – particularly in the absence of ISO27001 certification it is important that the University can demonstrate IGT compliance.

**Does the University have to do the IG Toolkit?**

Completion of IGT within universities is relatively new but increasingly recognised and expected.

IGT assessments **must** be completed by all organisations that fall under the responsibility of the Department of Health\(^8\).

In addition however there are additional circumstances (compulsory in Section 251 cases – use of identifiable patient information without patient consent\(^9\)) categories of organisations that must also carry out IG assessments to provide an assurance that they are adhering to good information

---

7 For advice on Data Management Planning see [www.le.ac.uk/researchdata](http://www.le.ac.uk/researchdata).
8 NHS organisations (acute trusts, ambulance trusts, mental health trusts, primary care trusts and strategic health authorities) including foundation trusts, adult social care, community pharmacies, dental practices, eye care services, general practices, DH arms' length bodies
governance practices. In September 2011 this was confirmed as including other organisations that have access to NHS patients and/or to their information:

All NHS organisations (and others with access to NHS patient information) should:

a. be using the NHS Information Governance Toolkit [https://www.igt.connectingforhealth.nhs.uk](https://www.igt.connectingforhealth.nhs.uk) to assess and publish details of performance

b. ensure all staff undertake appropriate information governance training annually as identified in the NHS Information Governance Toolkit [https://www.igt Learning](https://www.igt-learning.connectingforhealth.nhs.uk/igt/index.cfm)

Specific proposals and collaborations may result in requirement to complete IGT - if this happens contact [IGT@le.ac.uk](mailto:IGT@le.ac.uk) for advice and support.

Whether or not this in particular is demanded, good IG is a general requirement – fulfilling legal obligations, routinizing good practice and pushing for appropriate University services.

### 5. The College and IG Toolkit

Some research groups have been dealing with IGT for several years. With growing expectations however, in 2014-15 (the IGT year runs to 31 March) there was the formation of a College based IG Working Group, reporting to the CMBSP IT Advisory Committee. This group put together a successful College-wide IGT submission.

This was constructed as an ‘umbrella’ submission putting in place an IG framework and providing much of the evidence that other submissions can use – the expectation being that the IG Working Group will assist in further IGT submissions.

---

10 Taken from the joint letter from NHS England Chief Executive and ICO Commissioner, 5 September 2011.
Among things being developed or in place are:

- College-wide IGT submission
- IG Leads and Working Group
- Responsibility with College IT Advisory Committee
- IG/IGT web presence - [http://www2.le.ac.uk/colleges/medbiopsych/research/information-governance-igt](http://www2.le.ac.uk/colleges/medbiopsych/research/information-governance-igt)
- Approved IG Policy
- University Registrar as SIRO (Senior Information Risk Owner)
- Recommended Training

**IGT Registration**

As is commonly the case the decision was made to register the College under the ‘Hosted Secondary Use Team/Project’ IGT category:

**IGT (2012-13) Hosted Secondary Use Teams/Project (HSUT/P)**

For individuals, teams and their projects that **process NHS patient information** for the purposes of **non-direct care** e.g. clinical research activities and other related patient data analysis (public health planning). These individuals / teams are effectively **discrete sub-units or divisions of their host organisation** whose overall business interests may span a range of clinical and non-clinical activities e.g. **universities**, Public Health Teams hosted/employed by Local Authorities, commercial organisations. This requirement set enables such individuals / teams to **assess the adequacy of IG processes around their projects**.

**6. How do you provide evidence for the IG Toolkit?**

**When/how often**

Assessment and evidence gathering runs on a yearly cycle to 31 March, with the latest version of the toolkit usually being released in June.

Yearly submission of evidence should reflect on-going changes and improvements – with the requirement for an improvement plan.

An assessment can be started at any time after a new version of the IG Toolkit is released (June each year) but in all cases the final submission must be made online by 31st March each year (NHS organisations are also required to complete interim assessments during the year).

The work necessary to make improvements or to maintain compliance should be an on-going process and not left until the year end.

---

11 IG Policy, [http://www2.le.ac.uk/colleges/medbiopsych/research/information-governance-igt/docs/college-information-governance-policy](http://www2.le.ac.uk/colleges/medbiopsych/research/information-governance-igt/docs/college-information-governance-policy)

How

The University is IGT registered as organisation code ‘EE133832’.
All subsequent registrations should come beneath that registration code.

Following registration with the IG Toolkit via https://www.igt.hscic.gov.uk/ evidence is uploaded to the website against a set of standards applicable to the relevant organisation type.

The schedule of Standards varies according to the organisation type e.g. An Acute Trust has 45 standards, whilst the Hosted Secondary Use Team/Project has 14.

Note: Anyone can access this site and look at the standards and even the level of compliance for each organisation.

How does it work?
1. The toolkit consists of a number of standards.
2. Each standard is associated with detail of the subject area and what requirements - features/actions – need to be evidenced to satisfy the standard.
3. The organisation provides evidence against each of these standards.
4. Responsibility for this is given to an organisation “Administrator”, who can also grant others “Ownership” of particular standards and allow them to upload evidence.
5. For each standard according to specific evidence stated as required, and the evidence provided a compliance level is given – Not Applicable, 0, 1, 2, or 3.
6. The aim is to achieve an acceptable status of at least 2, and work to Level 3 for each.
Applicable IGT Standards for CMBSP as “Secondary Use Team/Project”:

**Hosted Secondary Use Team/Project Version 13 (2015-2016)**

Requirements List

<table>
<thead>
<tr>
<th>Req No</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>13-120</td>
<td>Responsibility for Information Governance has been assigned to an appropriate member, or members, of staff</td>
<td>View</td>
</tr>
<tr>
<td>13-121</td>
<td>There is an information governance policy that addresses the overall requirements of information governance</td>
<td>View</td>
</tr>
<tr>
<td>13-122</td>
<td>All contracts (staff, contractor and third party) contain clauses that clearly identify information governance responsibilities.</td>
<td>View</td>
</tr>
<tr>
<td>13-123</td>
<td>All staff members are provided with appropriate training on information governance requirements.</td>
<td>View</td>
</tr>
</tbody>
</table>

**Confidentiality and Data Protection Assurance**

<table>
<thead>
<tr>
<th>Req No</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>13-220</td>
<td>Personal information is only used in ways that do not directly contribute to the delivery of care services where there is a lawful basis to do so and objections to the disclosure of confidential personal information are appropriately respected</td>
<td>View</td>
</tr>
<tr>
<td>13-221</td>
<td>There are appropriate confidentiality audit procedures to monitor access to confidential personal information</td>
<td>View</td>
</tr>
<tr>
<td>13-222</td>
<td>All person identifiable data processed outside of the UK complies with the Data Protection Act 1998 and Department of Health guidelines</td>
<td>View</td>
</tr>
<tr>
<td>13-223</td>
<td>All transfers of personal and sensitive information are conducted in a secure and confidential manner</td>
<td>View</td>
</tr>
</tbody>
</table>

**Information Security Assurance**

<table>
<thead>
<tr>
<th>Req No</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>13-330</td>
<td>Policy and procedures ensure that mobile computing and teleworking are secure</td>
<td>View</td>
</tr>
<tr>
<td>13-331</td>
<td>There is an information asset register that includes all key information, software, hardware and services</td>
<td>View</td>
</tr>
<tr>
<td>13-332</td>
<td>Unauthorised access to the premises, equipment, records and other assets is prevented</td>
<td>View</td>
</tr>
<tr>
<td>13-333</td>
<td>There are documented incident management and reocontext procedures</td>
<td>View</td>
</tr>
<tr>
<td>13-334</td>
<td>The confidentiality of service user information is protected through use of pseudonymisation and anonymisation techniques where appropriate</td>
<td>View</td>
</tr>
<tr>
<td>13-335</td>
<td>There are adequate safeguards in place to ensure that all patient/client information is collected and used within a secure data processing environment (safe haven) distinct from other areas of organisational activity.</td>
<td>View</td>
</tr>
</tbody>
</table>

**In practice** increasing compliance levels tend to relate to:

- **0** - No evidence at all
- **1** - Responsibility for something being defined and documented, and/or the existence of something e.g. a policy.
- **2** – The thing has been made available, people have seen it, it has been discussed at meetings, and this has been documented.
- **3** – There are checks and reviews to prove it is understood and being applied.

Assessment relies on meaningful evidence being uploaded against specific requirements, and the website ticking off this evidence as existing, giving a compliance level. In affect this is self-assessment as you take the responsibility to say a document satisfies the requirement e.g. the document is actually the policy required, not a blank document.
7. What does this mean to me? – What do I have to do?

We all have general responsibilities to comply with local policy – including the College IG Strategy and Policy - the university Information Security Policy and relevant legislation, notably the Data Protection Act (see below).

There are numerous requirements and assurances regarding data handling, confidentiality and IT included within research proposal processes and data access requests e.g. IRAS forms. Advice should be sought as to how to appropriately respond including from the Information Governance Working Group - contact IGT@le.ac.uk.

There is also related on-line support and advice available:

- Information Governance - [http://www2.le.ac.uk/colleges/medbiopsych/research/information-governance-igt](http://www2.le.ac.uk/colleges/medbiopsych/research/information-governance-igt)
- Research Governance - [http://www2.le.ac.uk/colleges/medbiopsych/research/researchgovernance](http://www2.le.ac.uk/colleges/medbiopsych/research/researchgovernance)
- Research Data Management - [http://www.le.ac.uk/researchdata](http://www.le.ac.uk/researchdata)
- Information Assurance - [http://www2.le.ac.uk/offices/ias](http://www2.le.ac.uk/offices/ias)

If it is specifically requested or required, and when you are handling NHS data then there should be registration with, and submission of, evidence to the **Information Governance Toolkit**. The Information Governance Working Group has been specifically established to support IG improvement and to co-ordinate and assist in IGT registration and submission - contact IGT@le.ac.uk.

There are particular issues relating to the process of issuing Health and Social Care Information Centre (HSCIC) Data Sharing Agreements – researcher level agreements need to be co-ordinated with an institution level HSCIC Framework Contact - contact IGT@le.ac.uk.

As part of IGT compliance all College staff will be required to undergo appropriate training and will be advised what is necessary.
### The Data Protection Act Principles

<table>
<thead>
<tr>
<th>Principle 1</th>
<th>Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(a) at least one of the conditions in Schedule 2 is met, and</td>
</tr>
<tr>
<td></td>
<td>(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.</td>
</tr>
</tbody>
</table>

#### An explanation of Principle 1:
In practice, it means that you must:

- have legitimate grounds for collecting and using the personal data;
- not use the data in ways that have unjustified adverse effects on the individuals concerned;
- be transparent about how you intend to use the data, and give individuals appropriate privacy notices when collecting their personal data;
- handle people’s personal data only in ways they would reasonably expect; and
- make sure you do not do anything unlawful with the data.

#### What are the conditions for processing?
The conditions for processing are set out in Schedules 2 and 3 to the Data Protection Act. Unless a relevant exemption applies, at least one of the following conditions must be met whenever you process personal data:

- The individual whom the personal data is about has consented to the processing.
- The processing is necessary in relation to a contract which the individual has entered into, or
• Because the individual has asked for something to be done so they can enter into a contract.
• The processing is necessary because of a legal obligation that applies to you (except an obligation imposed by a contract).
• The processing is necessary to protect the individual’s “vital interests”. This condition only applies in cases of life or death, such as where an individual’s medical history is disclosed to a hospital’s A&E department treating them after a serious road accident.
• The processing is necessary for administering justice, or for exercising statutory, governmental, or other public functions
• The processing is in accordance with the legitimate interests of the parties involved, while not prejudicing the rights and freedoms of any individual.

The Caldicott Principles

The Principles were devised by the Caldicott Committee, which reported in 1997 following a review of patient-identifiable information. They represent best practice for using and sharing identifiable personal information and should be applied whenever a transfer of personal information is being considered.

<table>
<thead>
<tr>
<th>The Caldicott Principles</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Principle 1</strong>: Justify the purpose for using the information</td>
</tr>
<tr>
<td><strong>Principle 2</strong>: Only use identifiable information if absolutely necessary</td>
</tr>
<tr>
<td><strong>Principle 3</strong>: Use the minimum that is required</td>
</tr>
<tr>
<td><strong>Principle 4</strong>: Access should be on a strict need to know basis</td>
</tr>
<tr>
<td><strong>Principle 5</strong>: Everyone must understand their responsibilities</td>
</tr>
<tr>
<td><strong>Principle 6</strong>: Understand and comply with the law</td>
</tr>
</tbody>
</table>

CMBSP IG Working Group
26 August 2015

Version Control Table

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Author</th>
<th>Detail/Reason for Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Draft 0-3 \UoL_CMBSP_IGTIntro_v0-3.docx</td>
<td>26.08.2015</td>
<td>Andrew Burnham</td>
<td>IG Working Group input</td>
</tr>
<tr>
<td>Draft 0-2 \UoL_CMBSP_IGTIntro_v0-2.docx</td>
<td>18.08.2015</td>
<td>Andrew Burnham</td>
<td>Second Draft</td>
</tr>
<tr>
<td>Draft 0-1 \UoL_CMBSP_IGTIntro_v0-1.docx</td>
<td>26.02.2015</td>
<td>Andrew Burnham</td>
<td>First Draft</td>
</tr>
</tbody>
</table>

\UoL_CMBSP_IGTIntro_v0-3.docx A. Burnham, 26.08.2015