Content

1. What?
   What is ... Information Governance, IG Toolkit, Data, Personal Data, Sensitive Data

2. Why? – Information Governance

3. Who?
   Who has to carry out an information governance assessment?

4. When/How Often?
   When does the information governance assessment have to be done?

5. How?
   How do you provide evidence for the IG Toolkit?

6. Where is the College up to with IG?

7. What does this mean to me? – What do I have to do?

8. Issues and Challenges

9. References
1. What

What is Information Governance?

Information Governance is to do with the way organisations ‘process’ or handle information.

It covers personal information, i.e. that relating to patients/service users and employees, and corporate information, e.g. financial and accounting records.
(Ref. 1 - https://www.igt.connectingforhealth.nhs.uk/about.aspx).

It is therefore relevant when dealing with use of health care information (whether defined as, personal, sensitive, “person identifiable”, pseudonymised or anonymised).

What is “Data” (according the Information Commissioner’s Office)

Data means information which –

a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,
b) is recorded with the intention that it should be processed by means of such equipment,
c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,
d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68, or
e) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d).
(Ref. 2 - http://www.ico.gov.uk/for_organisations/data_protection/the_guide/key_definitions.aspx)

What is “Personal Data” (according the Information Commissioner’s Office)

Personal data 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. 2).

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.
(Ref. 1)
What is “Sensitive Personal Data” (according the Information Commissioner’s Office)

Sensitive personal data means personal data consisting of information as to -

- the racial or ethnic origin of the data subject,
- his political opinions,
- his religious beliefs or other beliefs of a similar nature,
- whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
- his physical or mental health or condition,
- his sexual life,
- the commission or alleged commission by him of any offence, or
- any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

(Ref. 2)

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.
(Ref. 1).

What is the IG Toolkit? (IGT)

The Information Governance Toolkit is a performance tool produced by the Department of Health (DH)/Health & Social Care Information Centre (HSCIC).

It draws together the legal rules and central guidance set out and presents them in one place as a set of information governance requirements.

Types of organisations described are required to carry out self-assessments of their compliance against the IG requirements.

The Toolkit consists of a number of standards against which assurance of compliance needs to be given.

2. Why? – Information Governance

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:

2. The common law duty of confidentiality.


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

3. Who?

Who has to carry out an information governance assessment?

Assessments must be completed by all organisations that fall under the responsibility of the Department of Health, these are:

- 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 (i.e. executive agencies such as the Medicines and Healthcare products Regulatory Agency; special health authorities such as the NHS Business Services Authority; and non-departmental public bodies such as the Health Protection Agency).

However,

There are additional categories of organisations that must also carry out IG assessments to provide an ‘assurance’ that they are adhering to good information governance practices. Examples of these are organisations that:

- have access to NHS patients and/or to their information
- provide support services directly to an NHS organisation
- have either direct or indirect access to NHS Connecting for Health services, including N3 - the NHS National Network.

As stated, these are examples of typical organisations and there may be other categories that are also required to provide IG assurance.

Depending on the services etc. provided, these organisations are referred to in the IG Toolkit as either a Commercial Third Party or an NHS Business Partner.

Among numerous Organisation types defined under the IG Toolkit:

- Hosted Secondary Use Team/Project - This is the category under which the College is registered
- Secondary Use Organisation
4. When/How Often?

When does the information governance assessment have to be done?

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

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/July 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.

5. How?

How do you provide evidence for the IG Toolkit?

This is done by uploading specific evidence defined against a set of standards applicable to the relevant organisation type via a website (Ref. 3. IGT Home Page - https://www.igt.connectingforhealth.nhs.uk/Home.aspx):

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.**

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

Standards are categorised as:

1. Information Governance Management
2. Confidentiality and Data Protection Assurance
3. Information Security Assurance
4. Clinical Information Assurance
5. Secondary Use Assurance
6. Corporate Information Assurance
Applicable IGT Standards for CMBSP as “Secondary Use Team/Project”:

<table>
<thead>
<tr>
<th>Req No</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>12-120</td>
<td>Responsibility for Information Governance has been assigned to an appropriate member, or members, of staff</td>
</tr>
<tr>
<td>12-121</td>
<td>There is an information governance policy that addresses the overall requirements of information governance</td>
</tr>
<tr>
<td>12-122</td>
<td>All contracts (staff, contractor and third party) contain clauses that clearly identify information governance responsibilities.</td>
</tr>
<tr>
<td>12-123</td>
<td>All staff members are provided with appropriate training on information governance requirements.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Req No</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>12-220</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>
</tr>
<tr>
<td>12-221</td>
<td>There are appropriate confidentiality audit procedures to monitor access to confidential personal information</td>
</tr>
<tr>
<td>12-222</td>
<td>All person identifiable data processed outside of the UK complies with the Data Protection Act 1998 and Department of Health guidelines</td>
</tr>
<tr>
<td>12-223</td>
<td>All transfers of personal and sensitive information are conducted in a secure and confidential manner</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Req No</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>12-330</td>
<td>Policy and procedures ensure that mobile computing and teleworking are secure</td>
</tr>
<tr>
<td>12-331</td>
<td>There is an information asset register that includes all key information, software, hardware and services</td>
</tr>
<tr>
<td>12-332</td>
<td>Unauthorised access to the premises, equipment, records and other assets is prevented</td>
</tr>
<tr>
<td>12-333</td>
<td>There are documented incident management and reporting procedures</td>
</tr>
<tr>
<td>12-334</td>
<td>The confidentiality of service user information is protected through use of pseudonymisation and anonymisation techniques where appropriate</td>
</tr>
<tr>
<td>12-335</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>
</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.
Typically an NHS Trust may be audited over several days to examine the detail of the evidence.

6. Where is the College up to with IG?

IGT Registration
For the last few years there have been two group/project IGT registrations. The College as a whole is now registered with the IG Toolkit as a “Hosted Secondary Use Team/Project”, and it is envisaged that Departments and/or research groups/projects will need to progress individual registrations.

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.

Organisations that make an application (under Health and Social Care Act (Section 251)) to the NIGB Ethics and Confidentiality Committee to the Data Access Advisory Group (DAAG) are required to provide IG assurance. If the host organisation has a current and satisfactory IGT assessment then the Team will not be required to complete an additional HSUT/P assessment. If the host cannot provide this assurance then the HSUT/P will be required to complete a satisfactory HSUT/P assessment. Large (non-hosted) organisations may need to complete Secondary Use Organisation view.

(Ref. 4 - https://www.igt.connectingforhealth.nhs.uk/resources/User%20Guide-Organisation%20Types.pdf)
7. What does this mean to me? – What do I have to do?

General
Responsibilities under IG and the IGT are outlined in the College IG Policy.

We all have general responsibilities to comply with local policy, the university Information Security Policy and relevant legislation, notably the Data Protection Act, be aware of the issues relevant to the health data context and to comply with the Caldicott Principles.

<table>
<thead>
<tr>
<th>The Data Protection Act Principles</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Principle 1</strong>: Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –</td>
</tr>
<tr>
<td>(a) at least one of the conditions in Schedule 2 is met, and</td>
</tr>
<tr>
<td>(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.</td>
</tr>
<tr>
<td><strong>Principle 2</strong>: Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.</td>
</tr>
<tr>
<td><strong>Principle 3</strong>: Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.</td>
</tr>
<tr>
<td><strong>Principle 4</strong>: Personal data shall be accurate and, where necessary, kept up to date.</td>
</tr>
<tr>
<td><strong>Principle 5</strong>: Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.</td>
</tr>
<tr>
<td><strong>Principle 6</strong>: Personal data shall be processed in accordance with the rights of data subjects under this Act.</td>
</tr>
<tr>
<td><strong>Principle 7</strong>: Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.</td>
</tr>
<tr>
<td><strong>Principle 8</strong>: Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.</td>
</tr>
</tbody>
</table>
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>

As part of IGT compliance all College staff will be expected to undergo appropriate training and will be advised what is necessary.
8. Issues and Challenges

Some of the issues to be aware of are:

- The IGT was originally set up for NHS organisations and in response to the clear need to improve practice and avoid information incidents.
- It relates most clearly to whole institutions such as NHS Trusts, which will be required, for example to have Trust-wide IG structures, and clear senior management responsibilities (such as a Caldicott Guardian and Senior Information Risk Owner, or SIRO).
- Universities do not fit into this organisational model – an on-going issue.
- The sector is in the process of interpreting and responding to IGT demands – few if any have the issue fully dealt with.
- There are a range of implications which include potentially the provision of costly IT infrastructure which appropriately handles this category of data.
- IGT has a clear relationship with the information security standard ISO27001, and much of its content relates to this ISO standard.
- As of October 2014 HSCIC began to demand ISO27001 certification and/or IGT compliance where HEI’s were in receipt of data.
- There is attempt to create a constructive relationship with HSCIC, influence IGT development (recognising HE issues) and provide guidance to the HE sector through the NHS-HE Forum IG Working Group.

9. References


See also:


\UoL_CMBSP_IGTIntro_v0-1.docx  A. Burnham, 26.02.2015

Information Commissioner’s Office, “Data Protection Technical Guidance, Determining what is personal data”,

**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 0-1</td>
<td>26.02.2015</td>
<td>Andrew Burnham</td>
<td>First Draft</td>
</tr>
</tbody>
</table>

CMBSP IG Working Group
26 February 2015