Introduction to Information Governance (IG) & the IG Toolkit

IG Working Group
The same old song?
The same old song?

London clinic leaks HIV status of patients

2 September 2015 | London

Dr Alan McGowan: "Not everybody on the list is HIV positive"

A London sexual health centre mistakenly leaked the details of nearly 800 patients who have attended HIV clinics, bosses have admitted.

The 56 Dean Street clinic in Soho sent out the names and email addresses of 780 people when a newsletter was issued to clinic patients.

Patients were supposed to be blind-copied into the email but instead details were sent as a group email.

Health Secretary Jeremy Hunt said the breach was "completely unacceptable".
The same old song?

NHS Trust receives largest ever data breach fine

Brighton and Sussex University Hospitals NHS Trust fined £325k after hard drives with highly-sensitive patient data were sold on eBay, but will appeal

An NHS Trust in Brighton has been served with the largest ever fine issued by the Information Commissioner, after hospital hard drives containing sensitive patient data were sold on eBay.

The hard drives contained medical records, home addresses and National Insurance numbers of "tens of thousands" of patients, the ICO said today, including children and patients treated by the Trust's HIV and Genito Urinary Medicine unit.
The same old song?

31 AUG 2012 NEWS

Cancer Care data breach compromises 55K patients

The data breach occurred after an employee’s notebook was taken from his locked car. Unfortunately, that computer contained a goldmine of exploitable information, including patient names and addresses, dates of birth, Social Security numbers, medical record numbers, insurance information and, Cancer Care said, possibly even clinical data about treatments. Employee data was also on the laptop.
The same old song?

University of York in student data breach on website

An investigation has begun at the University of York after personal data of 148 students was published.

Information including the students' mobile phone numbers, addresses and A-level results was made available.

The information could be accessed on a student inquiry page on the university's website.
Introduction to IG & IGT - Content

2,000 NHS patients’ records are lost every day with more than two million serious data breaches logged since the start of 2011

- Records have been mistakenly sold on eBay or dropped in the street
- Staff are also sending sensitive information to the wrong places
- One NHS Trust said information had been thrown into bins
- Fears they will fall into private hands - who will use them to make a profit

By SOPHIE BORLAND FOR THE DAILY MAIL
PUBLISHED: 00:18, 15 February 2014 | UPDATED: 13:40, 15 February 2014
Introduction to IG & IGT - Content

Health data really well managed – official
Conclusion?

There is no glamour in good information governance …

… but it means maintaining your reputation and keeping on doing your work.
Introduction to IG & IGT - Content

- What is Information Governance (IG)?
- When and why might IG be an issue for me?
- What we are doing
- What does this mean to me? – What can I do?
- Information Governance - Why?
- How the University can provide IG assurance
- The Information Governance Toolkit & the College
- How you use and provide evidence for the IG Toolkit?
- Responsibilities
What is Information Governance?

Research Data
- RD Management
- Sensitive Data
- Health data & IG Toolkit

Governance
- IG Framework
- Compliant Services
- Application of Knowledge & Practice

Information Security
- IS Mgmt System
- IS Mgmt
- Technical IS
The Breadth of Information Governance

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

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

- **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)

- **The process of generating IG Toolkit** submissions which relies on, and in turn drives development in the areas above.
What is Information Governance?

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

- Information Governance is the information aspect of Clinical Governance
- It concerns information security and confidentiality
- It 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
- It is relevant when dealing with use of health information (whether defined as, personal, sensitive, “person identifiable”, pseudonymised or anonymised)
What is Information Governance?

"My data are secure"
Research Sponsorship
IT Infrastructure & Services
Information Security Policy
Legislation, ISO standards
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?
When and why might IG be an issue for me?

Dealing with IG involves:

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

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

• the University providing an IG framework which needs to be applied in a practical context.
When and why might IG be an issue for me?
When and why might IG be an issue for me?

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?
What we are doing

• IG Working Group
• Contact point – IGT@le.ac.uk
• Co-ordination – Information Assurance
• Co-ordination – Research Governance
• IG Framework – Responsibility / IG Leads / SIRO
• IG Framework – Strategy / Policy
• IG Toolkit – College Registration/submission (annual)
• Training
What we are doing

• Research proposals / data sharing requests
• NHS-HE IG Working Group – national involvement
• Influence on IT developments (VPN, R:, standards, ISO27001)
• HSCIC communication / Data Sharing Contracts
• Standard advice / support
• College meetings / discussions
• Website – Information Governance, RDM
What does this mean to me? – What can I do?

- Good things you are already doing
- Much is in your control
- Knowing what you need to be aware of
- Avoiding common pitfalls
Handling Risk

- Reduce
- Transfer
- Avoid
- Accept
Handling Risk

- Less identifiable / only anonymised data (*reduce/avoid risk*)
- Reduce data transfers / secure method / encryption
- Encryption of data when working remote/mobile (*reduce risk*)
- Minimal staff access data (*reduce risk*)
- Use central data storage (*transfer risk to ITS*)
- Quantify, document and accept, but be aware of risk
Provide Assurance

- Quote policy
- Follow policy
- Raise awareness
- Do training
- Processes & procedures (SOPs)
- Existing Research Governance
- Documentation ("if it is not documented it hasn’t happened")
- Audit/Monitoring
Information Governance – Why?

A more robust and comprehensive approach to the management of data:

- active expectation of compliance with applicable legislation
- range of regulators
- those providing data such as HSCIC
- research funders
Information Governance – Why?

What is demanded:

• the ability to maintain confidentiality, integrity and availability of data, through people (with appropriate skills and training), processes and framework of responsibility, and technical means, alongside

• the means to actively evidence that this is a reality.
Information Governance – The means to address rules

- 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 Information Security NHS Code of Practice.
- The Records Management NHS Code of Practice.
Information Governance – The means to assurance

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.
How the University can provide IG assurance

• An IG Framework (defining responsibility etc.)
• Policies
• Processes e.g. Research Governance Sponsorship
• Services e.g. IT infrastructure
• Appropriately skilled staff who have undergone training
• Formal submission of evidence
How the University can provide IG assurance

- Research proposals and Data Management Plans (www.le.ac.uk/researchdata)

- ISO27001 certification - increasingly it is questioned whether there is University certification under the Information Security Management standard (there is no current University certification)

- Information Governance Toolkit (IGT) submission – particularly in the absence of ISO27001 certification it is important that the University can demonstrate IGT compliance.
What is the Information Governance Toolkit?

- The Information Governance Toolkit (IGT) is a performance tool produced by the Department of Health (DoH) and the responsibility of the 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
Does the University have to do the IG Toolkit?

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.igte-learning.connectingforhealth.nhs.uk/igte/index.cfm](https://www.igte-learning.connectingforhealth.nhs.uk/igte/index.cfm)
Does the University have to do the IG Toolkit?

- compulsory in Section 251 cases – use of identifiable patient information without patient consent
- other organisations that have access to NHS patients and/or to their information
- a collaborator demands it
- a data request results in it being required
The College and the IG Toolkit

• Some existing IGT work/submission
• IG Leads and Working Group
• Responsibility with College IT Advisory Committee
• 2014-15 first successful College-wide ‘umbrella’ IGT submission
• IG/IGT web presence - Approved IG Policy
• University Registrar as SIRO (Senior Information Risk Owner)
• Recommended Training
The College and the IG Toolkit

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.
The College and the IG Toolkit

College IG Toolkit
Hosted Secondary Use

- Departmental IGT
- Mandated Group/Project IGT
- Pre-existing IGT Submissions

College 'Umbrella': Framework, common standards, resources & templates

- Departmental Assurance
- Group/Project Detail
- Group/Project Detail
IGT Submissions – Sources of evidence

Complete IGT Submission

Department / Group Evidence

College Evidence

University Evidence
IGT Submissions – Sources of evidence

- Department / Group Evidence
  - a) Already do it
  - b) Document it
  - c) New practice / process / skills

- Complete IGT Submission

- College Evidence

- University Evidence
How do you provide evidence for the IGT?

- Talk to the IG Working Group
- Register for IGT
- Register under University of Leicester e.g. UoL-ResearchGroupX
- Evidence gathering through the year
- Evidence upload to IGT website
- Annual submission by 31 March
How do you provide evidence for the IGT?
How do you provide evidence for the IGT?

- The toolkit consists of a number of standards.
- Each standard is associated with detail of the subject area and what requirements need to be evidenced to satisfy the standard.
- The organisation provides evidence against each of these standards.
- Responsibility for this is given to an organisation “Administrator”, and via “Ownership” of particular standards.
- Each standard - compliance level is ‘Not Applicable’, 0, 1, 2, or 3.
- *The aim is to achieve an acceptable status of at least 2, and work to Level 3 for each.*
IGT Requirements (Hosted Secondary Use)

<table>
<thead>
<tr>
<th>Req No</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Information Governance Management</strong></td>
<td></td>
</tr>
<tr>
<td>13-120</td>
<td>Responsibility for Information Governance has been assigned to an appropriate member, or members, of staff</td>
</tr>
<tr>
<td>13-121</td>
<td>There is an information governance policy that addresses the overall requirements of information governance</td>
</tr>
<tr>
<td>13-122</td>
<td>All contracts (staff, contractor and third party) contain clauses that clearly identify information governance responsibilities.</td>
</tr>
<tr>
<td>13-123</td>
<td>All staff members are provided with appropriate training on information governance requirements.</td>
</tr>
<tr>
<td><strong>Confidentiality and Data Protection Assurance</strong></td>
<td></td>
</tr>
<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>
</tr>
<tr>
<td>13-221</td>
<td>There are appropriate confidentiality audit procedures to monitor access to confidential personal information</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>
</tr>
<tr>
<td>13-223</td>
<td>All transfers of personal and sensitive information are conducted in a secure and confidential manner</td>
</tr>
<tr>
<td><strong>Information Security Assurance</strong></td>
<td></td>
</tr>
<tr>
<td>13-330</td>
<td>Policy and procedures ensure that mobile computing and teleworking are secure</td>
</tr>
<tr>
<td>13-331</td>
<td>There is an information asset register that includes all key information, software, hardware and services</td>
</tr>
<tr>
<td>13-332</td>
<td>Unauthorised access to the premises, equipment, records and other assets is prevented</td>
</tr>
<tr>
<td>13-333</td>
<td>There are documented incident management and reporting procedures</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>
</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>
</tr>
</tbody>
</table>
How to make IGT easier

- Liaise with the IG Working Group – their job is to achieve compliance with you and to reduce duplication of effort: contact IGT@le.ac.uk
- Use College evidence – the College submission provides much of what any other IGT submission will need
- University IG web content - http://www2.le.ac.uk/colleges/medbiopsych/research/information-governance-igt
- University Research Governance web - http://www2.le.ac.uk/colleges/medbiopsych/research/researchgovernance
- University Research Data Management web – www.le.ac.uk/researchdata
Responsibilities

• General - **all** have responsibilities to comply with relevant legislation, notably the Data Protection Act, and the Caldicott Principles

• **All** team/project members – undergo recommended training

• **All** will contribute to evidence gathering:
  a) Contribute to documents
  b) Undertake training
  c) Review processes and practices
  d) Review technical systems
  e) Read and comply with advice/policy
  f) Demonstrate that you have read and are complying with advice/policy
  g) Undertake technical work to support agreed standards
What does this mean to me? – What do I have to do?

**Individual**
- Understand policies and issues, aware of the requirements, compliance day to day, responsible for records or data, and what they do with information they use
- IG Training

**IG Leads**
- Authoring the IG Policy
- Build Policy into standards & processes
- Ongoing compliance, IG Toolkit submission, Improvement Plan

**College IT Committee**
- IG Policy and framework approval, ensure resources to support the policy
- Ensure research meets legal responsibilities and adopts governance requirements
- IGT submission review and approval

**Institution**
- Institutional Policy and responsibility
- SIRO (Senior Information Risk Owner)
### Responsibilities

#### The Data Protection Act Principles

**Principle 1**: Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless—

(a) at least one of the conditions in Schedule 2 is met, and

(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

**Principle 2**: 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.

**Principle 3**: Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

**Principle 4**: Personal data shall be accurate and, where necessary, kept up to date.

**Principle 5**: Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

**Principle 6**: Personal data shall be processed in accordance with the rights of data subjects under this Act.

**Principle 7**: 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.

**Principle 8**: 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.
## The Caldicott Principles

| Principle 1: Justify the purpose for using the information |
| Principle 2: Only use identifiable information if absolutely necessary |
| Principle 3: Use the minimum that is required |
| Principle 4: Access should be on a strict need to know basis |
| Principle 5: Everyone must understand their responsibilities |
| Principle 6: Understand and comply with the law |
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:

- from those data, or

- 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.
What is “Sensitive Personal Data”? 

**Sensitive personal data** (according the ICO) means personal data consisting of information as to:

- the racial or ethnic origin of the data subject,
- their political opinions,
- their religious beliefs or other beliefs of a similar nature,
- whether they are a member of a trade union,
- their physical or mental health or condition,
- their 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.
References

- [http://www.bbc.co.uk/news/uk-england-london-34127740](http://www.bbc.co.uk/news/uk-england-london-34127740)