University of Oxford

Cancer Epidemiology Unit (CEU)
Policy and Procedure:
Confidentiality Audit

Version History

Version	Issue Date	Author	Description
1.0	June 2014	Lucy Wright	Initial version

Table of Contents

1 Policy management

This is a controlled document with read-only rights for unit staff and administrative rights for the Information Governance Lead.

This document is one of a number that describe the detailed policies and procedures that support the master Unit Information Governance Policy.

Title:	Confidential audit
Location:	v:\IG_policies
Owner:	Information Governance Lead
Approver:	Information Governance Committee
Review:	At least annually (and more frequently if required to make improvements in response to audits or incident management findings)
Applicability:	All Unit employees. All activities and processes that involve personal or possibly personal data performed by or under contract on behalf of the Unit. Electronic, paper and other hard copy records.
Interpretation:	Questions relating to the interpretation of this policy should be directed initially to the Information Governance Lead
Unit:	Cancer Epidemiology Unit (CEU) within the Nuffield Department of Population Health, University of Oxford

2 Organisation Roles and Responsibilities

The Unit Information Governance Policy describes the organisational structure, and defines key roles and responsibilities in relation to information governance, including:

- Unit Management
- Information Governance Committee
- Information Governance Lead
- Information Technology and Security Manager
- Senior Information Risk Owner

3 Policy wording

Convention	Description
Must	A policy provision that is mandatory
Should	A policy provision that is strongly encouraged but which may be ignored if there is good reason
May	A policy provision that should generally be followed
[…]	Text in [square brackets] does not form part of the policy but is provided by way of explanation or example

4 Abbreviations and definitions

<table>
<tr><th>Abbreviation</th><th>Description</th></tr>
<tr><td>Information Security Incident</td><td>An Information Security Incident is any event or occurrence that has resulted, or could have resulted, in the disclosure of confidential information to an unauthorised individual, a risk to the integrity of the system or data, or risk to the availability of the system.</td></tr>
<tr><td>Information Assets / Information Asset Owners</td><td>Information Assets are identifiable and definable assets owned or contracted by the Unit and which are ‘valuable’ to the business of the Unit. Information Assets may include the computer systems and network hardware, software and supporting utilities and staff that are required to achieve processing of this data, though Information Assets should not be seen as simply technical.

In general terms, Unit Information Assets fall into one of four categories:

<table>
<tr><th>Information Asset</th><th>Information Asset Owner</th></tr>
<tr><td>Clinical research study[1]</td><td>Principal Investigator</td></tr>
<tr><td>Administrative information[2]</td><td>Unit Administrator</td></tr>
<tr><td>IT infrastructure[3]</td><td>Director of Information Science</td></tr>
<tr><td>All other information</td><td>Unit Director[4]</td></tr>
</table>
[1] Examples include MWS, EPIC, DSW
[2] Examples include personnel files, unit accounts
[3] Examples include servers, firewall, networking
[4] or nominated deputy (e.g. Deputy Director)

The Unit must maintain a register of Information Assets and their Owners.

Further information is provided in the Unit Information Governance Policy.</td></tr>
<tr><td>Personal data</td><td>Personal data 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.
(http://ico.org.uk/for_organisations/data_protection/the_guide/key_definitions#personal-data)

The Health & Social Care Information Centre have published guidance on the drawing the line between personal and non-personal data.

http://www.isb.nhs.uk/documents/isb-1523/amd-20-2010/1523202010guid.pdf</td></tr>
<tr><td>Risk assessment</td><td>Risk is the potential for an unwanted event to have a negative impact as a result of exploiting a weakness. It can be seen as a function of the value of the asset, threats and vulnerabilities. The process of risk assessment is discussed as part of the Oxford University toolkit.
(http://www.it.ox.ac.uk/policies-and-guidelines/is-toolkit/risk-assessment/)</td></tr>
</table>

Abbreviation	Description
Sensitive personal data	Sensitive personal data means personal data consisting of information as to: (a) the racial or ethnic origin of the data subject, (b) his/her political opinions, (c) his/her religious beliefs or other beliefs of a similar nature, (d) whether his/her he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992), (e) his/her physical or mental health or condition, (f) his/her sexual life, (g) the commission or alleged commission by him/her of any offence, or (h) any proceedings for any offence committed or alleged to have been committed by him/her, the disposal of such proceedings or the sentence of any court in such proceedings. (http://ico.org.uk/for_organisations/data_protection/the_guide/key_definitions#personal-data)

5 Introduction

The Unit has a duty to protect the privacy of individuals, including (but not limited to) employees and study participants. Access to confidential information needs to be carefully monitored and controlled as failure to ensure that adequate controls to manage and safeguard confidentiality are implemented and fulfil their intended purpose may result in a breach of that confidentiality, therefore contravening the requirements of Caldicott, the Data Protection Act 1998, the Human Rights Act 1998 and the Common Law Duty of Confidentiality.

It is recognised that in general staff do not willingly abuse the information to which they have access, but the Unit has a responsibility to ensure that confidential information is protected. In particular, the increased use of electronic methods to store, process and transfer personal information and confidential data means that it is particularly important to guard against the possibility of information falling into the hands of individuals who do not have a legitimate right of access to it.

This policy sets out the assurance mechanism by which the effectiveness of controls implemented by the Unit is audited, areas for improvement and concern highlighted, and recommendations for improvements made.

6 Audits

6.1 Responsibilities

The Information Asset Owner must ensure that their Information Assets are audited on schedule and that any shortcomings that are identified are addressed in a timely fashion.

The Information Governance Lead must maintain the audit schedule and oversee their conduct and documentation.

6.2 Categorisation of Information Assets

The timing and nature of Confidentiality Audits depends on whether the Information Asset contains Confidential Information and is Active:

- If there is any doubt about whether an Information Asset contains Confidential Information, it must be treated as if it does.
- An Information Asset must be considered “active” if people are actively reviewing confidential data [e.g. management or analysis of an on-going or completed study].

6.3 Timing of audit

6.3.1 Active Information Assets that contain Confidential Information

In general, each relevant Information Asset (i.e. those that are active and contain confidential information) should be audited annually.

The Information Governance Lead should determine the exact frequency of audits depending on the risk. Audits should be more frequent if the Information Asset is particularly high profile, there are concerns about management of confidential data, or concerns are raised by the nature or number of Information Security Incidents. In some circumstances, the risk may be sufficiently high to require a “for-cause” or “prompt” audit. For those Information Assets that are low risk [e.g. well-contained or legacy assets with little or no confidential information, low levels of activity and no previous concerns or recent changes in practice], auditing may be less frequent.

6.3.2 Inactive Information Assets that contain Confidential Information

An asset that contains confidential information but is inactive must have an initial “full” audit but subsequent audits should be confined to checking that the inactive status is valid, that no changes in study or system architecture have invalidated previous controls and that the personnel access lists are valid.

6.3.3 Information Assets that do not contain Confidential Information

An Information Asset that does not contain confidential information must be audited to validate this statement. Further audits are not required unless the Information Asset acquires confidential information. The Information Asset Owner should confirm that this is the case on an annual basis.

6.3.4 Scheduling

The timing and nature of confidentiality audits must be determined by the Information Governance Lead, but should be done in consultation with the Information Asset Owner.

The Information Governance Lead should notify Information Asset Owners in sufficient time to allow scheduling issues to be identified and resolved. [In general, audits may be scheduled in January to October each year, with November and December reserved for delayed audits, report writing and scheduling for the following year. Information Assets may be listed for audit in the order that the previous year’s audit was completed. New Information Assets will be added to the start of the list.]

The Information Governance Lead should make reasonable efforts to accommodate events such as other audits, data monitoring exercises, etc., that may impact on the Information Asset Owner and staff. In the interests of efficiency, audits may be scheduled together [e.g. for studies involving similar personnel and similar information processing methods] and may be spread through the year to avoid an undue peak load.

The Information Asset Owner may request that an audit be performed earlier than scheduled. [Compliance with this request will be subject to resources being available.]

The Information Asset Owner may submit a request to defer the audit to the Information Governance Lead, who must determine whether this request will be accommodated. Only one such request is allowed per asset per year, and an audit should not be deferred into the following calendar year.

Failure to complete an annual audit is considered a major Information Security Incident, and must be reported as such.

6.4 What an Audit Should Check

Audits must be conducted against the Unit policies, including the Unit Information Governance Policy and the Unit Information Security Policy (which embody relevant UK legislation and University regulations and policies), and any specific Information Asset policies and procedures [e.g. protocol, data exchange agreements, study-specific standard operation procedures].

In particular, audits should review and expect to find evidence of the following with respect to the Information Asset:

- clear documentation listing current users who have access to specific directory areas
- clear documentation listing current users who have access to project databases
- appropriate, documented procedures for removing access from users who no longer need it
- passwords are of an appropriate complexity and expire appropriately
- no evidence of inappropriate shared logins
- resolution of previous Information Governance Incidents (including issues identified at previous Confidentiality Audits) and completion of any resultant recommendations or required actions (including training and disciplinary issues)
- provision of appropriate staff training with respect to Information Governance (including relevant confidentiality and Information Security Incident Reporting and Management policies and procedures)
- access to physical areas containing personal information is restricted appropriately, including server rooms, mail handling areas and fax machines (if relevant)
- secure storage of and appropriately controlled access to filed hard copy personal information
- where information is removed from the workplace - has authorisation been gained either for long-term or short term removal?
- portable electronic media, including laptop computers, are appropriately secured (including encryption)
- secure disposal of confidential waste
- appropriate arrangements for data transfer and sharing
- appropriate monitoring of any third parties [e.g. subcontractors, research collaborators] which store or process Confidential Information relating to the Information Asset

6.5 Physically Dispersed Studies

Where a clinical study or other Information Asset is split across multiple geographical sites, it may be sufficient to establish that appropriate monitoring occurs at these sites to address the questions in Section 6.4. A lack of appropriate monitoring must be considered as a major noncompliance issue (Section 7.1).

7 Reporting

Once the audit has been completed a report must be produced. This should include:

- Details of the audit (including the date and the name of the auditor)
- A summary of the findings
- Details of any non-compliance
- Recommendations of any actions (clearly indicating those that are mandatory as opposed to for consideration)

7.1 Non Compliance

Noncompliance issues should be adequately documented in the audit report to allow for remedial action. Minor noncompliance issues may be addressed as part of the reporting process. Major noncompliance issues must be raised as an Information Security Incident.

The Information Governance Lead and the Information Asset Owner must discuss the audit findings and should agree the corrective actions required, the owner of each issue and the timescale for corrective action.

Disagreements over the report (including any findings and recommendations) must be referred to the Information Governance Committee for resolution.

8 Training

All staff must receive training in Information Governance at induction and annually thereafter. This should include policies and procedures relevant to their role. Requests for additional training or guidance should be discussed with line managers or addressed to the Information Governance Lead.

9 References

9.1 Unit Policies

Policy
Information Security Policy v:\IG_policies
Information Governance Policy v:\IG_policies

9.2 University policies

Policy
University of Oxford policy on Data Protection http://www.admin.ox.ac.uk/councilsec/compliance/dataprotection/
University of Oxford Information Security Policy http://www.it.ox.ac.uk/policies-and-guidelines/information-security-policy
University of Oxford Guidance on Risk Assessment http://www.it.ox.ac.uk/policies-and-guidelines/is-toolkit/risk-assessment/

9.3 External references

Policy
London Ambulance Service Confidentiality Audit Procedure (used as a model for this policy) http://www.londonambulance.nhs.uk/talking_with_us/freedom_of_information/classes_of_information/idoc.ashx?docid=2df68aec-bc6a-47ce-8d19-f08924489e6a&version=-1