University of Oxford

Cancer Epidemiology Unit (CEU)

Policy:
Information Security Incident Reporting and Management

Version 1.0

Version History

Version	Issue Date	Author	Description
1.0	07-Oct-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 Cancer Epidemiology Unit Information Governance Policy.

Title:	Information Security Incident Reporting and Management
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 activities performed that may impact on compliance with the Unit's Information Governance Policy
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 Committee
- Information Governance Committee
- Information Governance Lead
- IT and Information 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 (see section 6).</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 Strategy</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, networks
[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 potential for an Information Security Incident exists in any organisation, and such incidents need to be carefully managed to ensure that the damage, if any, is limited and that "lessons learned" are propagated forward to reduce the opportunities for future problems.

6 What is an Incident?

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.

i. Any reported or suspected breach of data protection or confidentiality must be treated as an Incident, whether it is well founded or not. This includes, but is not limited to:
    - loss or other exposure of participant or personnel records in electronic or paper form
    - general concerns about the IT infrastructure, even if they have not led to a demonstrable breach
    - lost or stolen hardware
ii. All audits conducted by external agencies or "for-cause" (including internal audits) must also be treated as Incidents for management and reporting purposes, and to ensure that "lessons learned" are propagated.
iii. Requests for significant amounts of time spent (if the request is expected to involve more than a half day's work) will also be treated as an incident for reporting purposes as it is presumed to indicate a weakness in the understanding of current procedures.

7 Incident management

7.1 Initial Reporting

Staff must report actual or suspected breaches to their line manager, and either directly or through their line manager to the Information Asset Owner and the IT & Security Manager. Urgent reports should be in person, where possible, to ensure timely resolution.

7.2 Responsibility

The IT & Security Manager is responsible for the general management of Incidents and may appoint an Incident Manager for a particular Incident. In case of absence, the Unit Director should appoint an alternative to oversee the investigation and response.

7.3 Basic Procedure

The Incident Manager should:

- establish whether an incident has, in fact, occurred;
- evaluate the extent of the damage or risk to the organisation as a result of the incident;
- ensure that timely and appropriate remedial action is followed;
- establish where the responsibility for the incident lies;
- review procedures to reduce the risk of the incident occurring again, keeping a record of lessons learned and propagating this information to relevant parties;
- ensure that, where practical, evidence is secured if future legal action be likely;
- compile an incident report.

These points may not always be pursued in the order listed. Where there is a conflict, the prevention of further data loss and the security of personal data must be the priorities.

7.4 Recording Details

The IT & IS Manager is responsible for keeping a record of all incidents. Each record should eventually include:

- date of incident (if identifiable);
- location of incident (if identifiable);
- details of staff involved (if identifiable and applicable);
- description of incident (including the type of event and the risk to the Information Asset and the Unit);
- description of any contributing factors;
- an account of remedial action taken following the incident (including immediate actions taken to reduce/eliminate the risk);
- recommended corrective action (including responsibility and timeline) to be taken to prevent a reoccurrence of this incident or similar incidents;
- a summary of any disciplinary or legal aspects;
- details of all onward reporting (e.g. University Network Security team, University Data Protection Officer, the police).

7.5 Summary Reporting

The IT & Security Manager must provide summary reports as follows:

7.5.1 Confidential review

Individual events should be summarised and provided to the Information Governance Committee for review at least annually. These summaries may contain confidential information.

7.5.2 Unit Management Review

An overall summary should be reported to the Unit Management on an annual basis. Individual events may be reported in more detail for discussion and education (but in doing so, any confidential information that may exist in the Incident Report should not be disclosed).

7.6 Disciplinary, legal and other considerations

An Incident involving the potential for disciplinary or other legal action must be treated with care to ensure that all parties are appropriately represented and that their privacy is respected as far as practical. The Unit Director must be involved in any such investigations. It should be remembered that a reported breach may not be an actual breach and care must be taken to avoid reputational damage to any party.

Unit personnel will only report potential Incidents (“near misses”) if they feel secure in doing so. It is important that the Incident Investigation is courteous and avoids embarrassment where possible.

8 Training

All staff must receive training in Information Governance at induction and annually thereafter. This must include Incident Reporting and Management 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/