University of Oxford

Cancer Epidemiology Unit (CEU)

Policy:
Protection and Transmission of Personal Information

Version 1.0

Version History

Version	Issue Date	Author	Description
1.0	08-Oct-2014	Lucy Wright	Initial version

Table of Contents

1 Policy management 4
2 Organisation Roles and Responsibilities 4
3 Policy wording 4
4 Abbreviations and definitions 5
5 Introduction 7
6 Data Protection Act 7
7 Processes for Sending and Receiving Data 7
7.1 General Considerations 7
7.2 Scope of this policy 8
7.3 Post 8
7.4 Fax 8
7.5 Telephone 9
7.6 Text Message 9
7.7 Electronic 9
7.7.1 Introduction 9
7.7.2 Appropriate Levels of Encryption 9
7.7.3 Encryption passwords 10
7.7.4 Key pairs and similar 10
7.7.5 Self-decrypting archives 10
7.7.6 Other notes 10
7.7.7 Receipt of electronic data 10
8 Information exchange agreements 11
9 Information Security Incident Reporting and Management 11
10 Audit and Record Keeping 11
10.1 Duties of the Information Asset Owner 11
10.2 Duties of the Information Governance Lead 11
10.3 Simplified Record Keeping 12
11 Training 12
12 References 12
12.1 Unit Policies 12
12.2 University policies 13
12.3 External guidance documents 13

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:	Protection and Transmission of Personal Information
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 performed by or on behalf of the Unit under contract. The Unit bears no responsibility for the actions of other entities not under contractual control, particularly in respect to how they manage their data under the Data Protection Act (or equivalent). However, once data fall under the control of the Unit, the data must be protected appropriately (regardless of nature, location or jurisdiction of the source). This policy should be applied to data related to any individual, regardless of vital status (alive or dead).
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 & 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.</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, 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 Unit has a duty to protect the privacy of individuals, including (but not limited to) employees and study participants. Furthermore inappropriate disclosure (whether inadvertent or deliberate) may have devastating consequences for the Unit, including fines of up to £500,000 (under the Data Protection Act) and serious damage to the Unit's reputation and research activities.

Many clinical studies routinely exchange data with other organisations (e.g. acquiring clinical data). However, it is important to remember that other activities (such as human resources) may also deal with extensive personal data.

This policy describes the procedures that must be applied to all transfers and transmissions of personal data to individuals or organisations external to Unit.

This policy is applicable to all Unit operations. However, since individual jurisdictions may apply additional requirements, compliance with this policy should not be taken as evidence of local legislative compliance.

The security of data "at rest" is discussed in the Information Security Policy.

6 Data Protection Act

The Unit must comply with the Data Protection Act (1988) and associated Codes of Practice issued by the Information Commissioner's Office and as part of the University of Oxford, the Unit must comply with the University policy on Data Protection. University of Oxford holds the Data Protection Registration number Z575783X.

The Data Protection Act makes no reference to the source of the data or the nationality of the individuals referenced therein. Therefore all personal data must be considered within scope. (For example, at the point at which data from other countries are transferred to CEU, the data fall under the requirements of the UK Data Protection Act.)

7 Processes for Sending and Receiving Data

7.1 General Considerations

The Information Asset Owner, or a nominated deputy, must give written or electronic consent for data transfer. [Note: This could be achieved through a written policy or procedure specific to the Information Asset that has been formally approved in writing or electronic form by the Information Asset Owner.]

Before exchanging data with an external source, consideration must be given to:

- whether the data can be rendered non personal by omitting certain columns [e.g. where the names are not a requirement] or reformatting the data [e.g., changing names to initials]
- whether the number of records sent is appropriate [e.g. a clearer understanding of the recipient's needs may make it possible to reduce the number of records transmitted]
- whether the data can be de-identified (anonymised or pseudo-anonymised) before transmission
- whether the target of the data transmission is governed by appropriate legislative or contractual controls to ensure that data protection is maintained
- when data is received, consideration must be given to how it will be promptly secured

Personal data must not be transferred to an environment which lowers the protection of the data.

7.2 Scope of this policy

If a data set contains personal information, its transmission must comply with the provisions set out in this policy.

If a data set demonstrably does not contain personal data, its transmission is outside the scope of this policy, but consideration should be given to whether there are any negative consequences of treating the data as personal, regardless.

If there is doubt (perhaps because the dataset is extensive, complex or poorly understood) the data set must be treated as if it contained personal information.

7.3 Post

Postal communications containing personal information must be sent in a sealed envelope, addressed to a named recipient or post holder [e.g. “Practice Manager”]. Where window envelopes are used, care must be taken to ensure that the addressee information remains visible and to avoid confidential information becoming visible as the contained paper shifts around.

Postal communications containing sensitive information should be marked “private and confidential”.

The sender must ensure that the packaging is suitable, remembering that packages may not be treated with care. The packaging should indicate a return address.

Information Asset Owners who are sending postal communications must have procedures in place to ensure that only the correct documents are placed inside the envelope [e.g. to ensure that a second person’s data is not inadvertently sent out in the same envelope as well.]

Postal communications containing “bulk” information should be sent by a tracked delivery service. [“Bulk” is difficult to define as different target organisations have different thresholds. Individual Information Asset Owners should discuss with the Information Governance Lead and document the outcome decision.]

The Information Asset Owner must perform routine audits of the effectiveness of these procedures.

Personal information received at the Unit by post must not be opened in public areas and must be stored securely (see the Unit Information Security Policy for discussion of storage of data at rest).

7.4 Fax

The transmission of personal data by fax should be avoided [as the use of fax machines is one of the most common sources of confidentiality breaches].

If personal information is to be sent by fax, there must be a risk assessment justifying why no other method of data transmission is practical.

Personal data must not be sent by fax unless it has been established that:

- The target fax machine is sited in a secure area away from unauthorised viewing.
- Access to the target fax machine is limited to authorised staff.
- The correct target fax number has been ascertained and checked.
- The recipient is available to receive the fax. [It is not acceptable for the information to sit on the fax machine for an extended period of time.]

Personal data received by fax at the Unit must be stored securely (see the Unit Information Security Policy for discussion of storage of data at rest), and the above points must be applied equally to an arrangement where faxes containing personal data are received.

7.5 Telephone

When receiving calls:

- Before discussing personal or sensitive data with an external caller, the recipient of the call must establish the caller's identity and authority, preferably by asking for some secondary item of information [e.g. the participant's date of birth]. Recipients must not discuss personal or sensitive data on the sole basis of an ID number.
- In the event that the caller does not have clear authority, but there are clear clinical requirements, the recipient should have the permission of the Information Asset Owner before disseminating personal information, or be acting according to an agreed SOP.
- If there is doubt as to the identity of the caller, the recipient should arrange to call back, allowing for time to check details.

When making calls:

- The caller must take care to establish the identity of the person with whom they are speaking.
- Messages left on answering machines, voicemail (or similar) or with other individuals must be kept to a minimum of personal information.

In General:

- Care should be taken to ensure that discussions are not overheard by other people who do not have a "need to know".
- Discussions should not take place in a public area.
- Telephone calls that result in the exchange of personal information should be documented.

7.6 Text Message

Personal information must not be sent by SMS/Text message.

Depersonalised messages are permitted [Example: messages containing appointment details, but not personal details].

7.7 Electronic

7.7.1 Introduction

Electronic transmission of data includes email, web, CD, DVD and other means of transmitting data electronically. The Unit engages with a wide selection of other organisations, each of which has their own rules on electronic transmission of data. As such, it is not possible to specify solutions, only preferred approaches and minimum standards.

7.7.2 Appropriate Levels of Encryption

Bulk data containing personal identifiers must be encrypted in transit. If there is no available mechanism, it is not permissible to send records unencrypted.

Encrypted personal data to be transmitted electronically must be encrypted to a level at least equivalent to AES-128.

Where practical, personal data to be transmitted should be encrypted to a level equivalent to AES-256 or better (or equivalent).

Individual records containing limited personal data and no directly sensitive data may be sent unencrypted provided a suitable risk assessment has been carried out and agreed with the Information Governance Lead, and where the extent of the personal data is limited.

[Examples of this include email newsletters for study participants or email invitations to join a study sent to individuals].

7.7.3 Encryption passwords

Where an encryption technique requires a password:

- Passwords must conform to the minimum standards set out in the Information Security Policy.
- Passwords must not be transmitted with the encrypted file.
- Passwords should be transmitted by an alternative mechanism to that used for the encrypted file.

7.7.4 Key pairs and similar

Where the encryption of data relies on the exchange of asymmetric "keys" [e.g. PGP key exchange], care must be taken to limit the access to the decryption key.

7.7.5 Self-decrypting archives

The use of self-decrypting archives should be avoided. Where self-decrypting archives are used, they must conform to the rules for transmission of electronic data.

7.7.6 Other notes

Care must be taken when selecting the target for any email containing personal data. [Many email programs helpfully offer a selection of email addresses that match the first few letters typed, and selecting the wrong entry is easy. Similarly, large organisations such as the NHS may have a number of individuals with very similar names and email addresses.]

Where practical, a target email address should be validated by an initial email exchange with no personal data attached.

Some data handling packages maintain an audit of changes internal to the document. Consideration must be given to the possible presence of such audit records when sending apparently depersonalised records.

Where electronic data is to be sent via physical media (e.g. DVD), the provisions of section 7.3 should also be considered.

7.7.7 Receipt of electronic data

It is not possible to control how external entities send data to CEU, although Information Asset Owners should encourage external entities to transmit data in a secure manner.

An Information Asset Owner must not enter into a data sharing agreement that they know to be inappropriate under this policy.

Received personal data, however transmitted, must be stored securely on arrival (see the Unit Information Security Policy for discussion of storage of data at rest).

In instances where personal data is transmitted insecurely by an external entity, this must be raised as an Information Security Incident (see the Unit Information Security Incident Reporting and Management Policy). Consideration should be given as to what form of feedback to the external entity is appropriate.

Where the received data is on physical media, consideration should be given to how to secure the physical media, and whether to retain or destroy the physical media once the data set has been transcribed or imported into a secure location.

8 Information exchange agreements

Information Asset Owners intending to send personal data to an external entity must ensure that there are appropriate agreements in place to ensure that the protection that the Unit affords the data is not degraded. Such agreements should be legally enforceable.

Information Asset Owners intending to transfer personal data must register the process with the Information Governance Lead (see section 10) and must seek the advice of the Unit Administrator (who may involve the University Research Services for contractual or legal input).

The Information Asset Owner must be able to demonstrate that the external entity understands and agrees to their obligations. For data transferred within the European Economic Area, this is implicit in the European Data Protection legislation, but it is preferable to gain explicit proof. For data transferred outside of the European Economic Area, the Information Asset Owner must consider the legal implications.

Agreements should be between named legal entities and should specify:

- names of the Information Asset Owner both within the Unit and at the external organization
- how long the external body may hold the data
- how the data should be disposed of
- what provisions (if any) exist for the onward transmission of the data, and
- minimum levels of protection that must be afforded the data.

Transfers of personal data between different aspects of a study may be governed by Binding Corporate Rules.

9 Information Security Incident Reporting and Management

Requirements for Information Security Incident Reporting and Management are set out in the Unit Information Security Incident Reporting and Management Policy.

10 Audit and Record Keeping

10.1 Duties of the Information Asset Owner

Information Asset Owners:

- must ensure that appropriate contracts, authorisations, consent and ethics related issues are in place.
- must inform the IT & Security Manager of intended transfers of personal data, including the type(s) of personal data, the entity to which the data will be sent, the mechanism of transmission and whether this is considered to be a “one off” or a repeated instance. A transfer of data between different aspects of a single study does not need to be notified to the Information Governance Lead, except in overview, provided there are measures to ensure data protection. Such measures should be recorded in study documentation such as the System Level Security Plan. [Example: a study may transfer data between a Central Coordinating Office and a Local Investigator where the data relates to that investigator’s patients.]
- must track individual data exchanges
- must not authorise the transfer of personal data without a sign off from the IT & Security Manager

10.2 Duties of the IT & IS Manager

The IT & Security Manager:

- must maintain a register of transfers.
- must audit the proposed transfer for compliance with relevant procedures and regulations.
- should periodically initiate an audit to ensure continued compliance.

10.3 Simplified Record Keeping

To simply record keeping:

- An Information Asset Owner, or the IT & Security Manager, may specify a data transfer mechanism that will be used for transfers to multiple entities. Although each additional target entity must be recorded, continuous re-inspection of the mechanism is not required.
  [Example: An Information Asset Owner proposes a transfer of personal data to an organisation. The IT & Security Manager inspects the proposed transfer and agrees the target and mechanism. The Information Asset Owner proposes a transfer of information to a second organisation under the same mechanism as the first. The IT & Security Manager should consider whether there are implications arising from the second organisation (perhaps they are in a different jurisdiction), but does not need to examine the exchange mechanism in detail.]
- The IT & Security Manager should specify a list of "trusted targets" where the transfer mechanism is already validated. The Information Asset Owner must notify the IT & Security Manager of an agreement to transfer data to this entity "under the usual arrangements", but continued re-inspection of the mechanism is not required.
  [Example: Many Information Asset Owners will transfer information to the Health & Social Care Information Centre in order to receive death certificates. Since the Health & Social Care Information Centre has a specified mechanism to which all Information Asset Owners must adhere, it is not a requirement to continuously inspect and test the mechanism of transfer.]
- Transmission of personal data between central databases and program interfaces used only by study team members does not need to be recorded by the IT & Security Manager.

11 Training

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

12 References

12.1 Unit Policies

Policy
Information Security Policy v:\IG_policies
Information Governance Policy v:\IG_policies
De-identification

v:\IG_policies
Information Security Incident Reporting and Management v:\IG_policies

12.2 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/

12.3 External guidance documents

Policy
The BMA Confidentiality Toolkit (discusses the release of clinical data): http://bma.org.uk/practical-support-at-work/ethics/confidentiality-tool-kit
“Binding Corporate Rules” and International Data Transfer are discussed in https://www.igt.hscic.gov.uk/KnowledgeBaseNew/ICO_International%20Transfers_v3.pdf