Confidentiality Policy

ESPE DSD REGISTRY

1. Introduction

1. The NeSC places the highest priority on maintaining the confidentiality of the information that it holds. It is essential that patient identifiable information is handled, processed and released in a strictly controlled manner. This document sets out the NeSC policy for the management of confidential information.

2. The EuroDSD project does not involve the collection of patient identifiable information in the Registry.

3. Overall responsibility for information security rests with the NeSC Director [**Prof Richard Sinnott**]. All staff are required to be familiar with the contents of this policy and to strictly adhere to it.

4. Any member of staff who at any time has difficulty in understanding the rules or thinks that they are insufficient or are being misapplied has a positive duty to do something about it. In case of doubt, the NeSC Director or a member of the senior management team should be consulted at the earliest opportunity.

5. Failure to observe these rules may lead to appropriate disciplinary action being taken which, in serious cases, may lead to dismissal.

6. The policy is complimentary to other NeSC policies and should be used in conjunction with them.

7. The policy shall be reviewed annually.

2. Confidentiality measures

1. All staff receiving and using personal information shall be bound by a legal duty of confidence.

2. NeSC shall maintain the same standards of confidentiality as customarily apply to the doctor-patient relationship. This obligation extends indefinitely, even after the death of the patient.

3. All staff shall sign a “Confidentiality Undertaking Form” (see Appendix “A”) as part of their contract of employment.

4. The term "Confidential Information" shall apply to any information relating to identifiable individual patients, clinical staff or practitioners held in a document, on microfiche/microfilm or magnetic medium (disc or tape) or other machine readable electronic form.

5. NeSC staff may come into contact with confidential information and/or handle a large amount of personal data on patients or clinical staff. All personal data shall be regarded as confidential.

6. If work is contracted to a 3rd party who in the course of their work may require access to confidential or patient identifiable data, the 3rd party will be required to sign the appropriate NeSC Confidentiality Agreement for external contractors.

3. Compliance with legislative and contractual requirements

NeSC has obligations to maintain confidentiality under the following legislation and guidance:

3.1. The Data Protection Act

The Data Protection Act (1998) lays down regulations for the handling of personal data. For all such data it is essential to abide by the eight principles which govern the care and use made of the data. In addition to these principles there are other conditions which have to be met and these are specified in the schedules of the act, full details are available at: http://www.legislation.hmso.gov.uk/acts/acts1998/19980029.htm .

Before personal data are held on computer, it is necessary to notify the Office of the Information Commissioner. Copies of NeSC registrations are held by the NeSC's Data Controller [**Dr John Watt**] and these should be checked regularly to ensure that all uses and especially disclosure of personal data are covered. NeSC is covered under the registration for the employing authority, (**University of Glasgow**). The NeSC Director takes overall responsibility for data protection within NeSC.

Failure to register personal data or knowingly to use data other than as registered will constitute an offence under the Act which may result in NeSC and/or individual employees being prosecuted and fined. Also, it is essential that the registrations are kept up to date, and the Director is responsible for informing the Data Controller regarding any new uses.

3.2. The Caldicott Guidance

In 1997 the Caldicott Committee introduced stringent guidelines in the recording, access and use of personal data within the NHS. All NHS organisations have a Caldicott Guardian. The NeSC Caldicott Guardian is **Dr Richard Copeland**, who delegates responsibility to the NeSC Director.

The six principles provided by the Caldicott Report are the baseline for good practice:

1. Justify the purpose for using confidential information
2. Only use it when absolutely necessary
3. Use the minimum that is required
4. Access should be on a strict need to know basis
5. Everyone must understand his or her responsibilities
6. Understand and comply with the law

3.3. Information flows

There is an annual review of the justification of flows of any patient identifiable information.

4. Release of Data

4.1. Release of identifiable data

Individual records are identifiable if name, address, NHS No. or postcode is present; any other information is present which, in conjunction with other data held by or disclosed to the recipient, could identify the patient. This also applies to NHS numbers or other unique numbers for which recipients of the data have access to the "key" to trace the identity of the patient using this number.

4.1.1. Controlling the release of identifiable data

The control of the release of identifiable data depends on the circumstances.

- Data subjects (patients) are entitled, under certain conditions, to examine their own records under the provisions of the Data Protection Act (1998).
- Medical practitioners may be given access to data on patients for whom they are responsible. This would normally mean that they have diagnosed or treated the condition which has been registered.
- Designated individuals in organisations providing care for the patient at any point in the clinical journey.
- Designated individuals for the purposes of audit and monitoring.
- Regional Directors of Public Health, Strategic Health Authority Directors of Public Health for the purpose of investigating specific public health concerns about service quality.

All other requests for patient identifiable data including all new requests for identifiable data for research require either patient consent or exemption under the Health & Social Care Act (2001).

4.1.2. Release of 'potentially' patient identifiable data

Aggregate data may also be identifiable in practice if linked formally or informally with other information, for example in small communities.

As a general rule, the following categories should be regarded as being potentially identifiable data:

- Individual records even if they do not include variables, such as names, full postcodes, and dates of birth which would make them obviously identifiable
- Tabular data, based on small geographic areas, with cell counts of fewer than five cases/events (or where counts of less than five can be inferred by simple arithmetic)
- Tabular data containing cells that have underlying population denominators of less than 1,000

As a general rule, the following categories should be regarded as potentially identifiable data for small geographic areas:

- Those areas where the total denominator population is less than that of a Primary Care Trust, e.g. wards or aggregations of wards. (The smallest PCT in England has a total population of approximately 62,000 i.e. 1,550 if divided into 40 single sex, 5-year age groups assuming an equal size distribution)
- Any geographic area (e.g. local authority) which, when released, may provide information regarding small population non-contiguous areas (“slivers”) when combined with Primary Care Trust information. These should be regarded in the same way as ward level data
- Any geographic area when publication in five-year age groups between 0 and 24 years is required. In this age range, particular scrutiny should be paid to tabulations and appropriate aggregations used. (Due to the rarity of many conditions in children and young adults, there may be a non-negligible risk of information disclosure by for any geographic area)

4.1.3. Release of data identifying individual clinicians

Data shall be released to:

- the named clinician;
- designated individuals as identified by the management group of the Register.

4.2. Requests for identifiable data

All releases of data must be approved by the NeSC Director and shall be requested in writing.

Releases of both identifiable and potentially identifiable data are governed by the following principles:

- the intended use(s) of the data should be stated clearly in writing

- the use(s) of the data should be justified and the data should not be used for any other purpose(s)
- the registry should not release data that are more detailed than necessary to fulfil the stated purpose
- the data should not be passed on to other third parties or released into the public domain
- the data should be kept securely for the period of time that can be justified by the stated purpose, and then destroyed
- no attempt should be made to identify information pertaining to particular individuals or to contact individuals (unless patient consent has been obtained via the patient's clinician)
- no attempt should be made to link the data to other data sets, unless agreed with the data providers
- any public domain reports or papers resulting from analyses of the provided data should be shared prior to publication with the registry supplying the information.
- recipients of data should be aware of their responsibilities, and should sign an agreement to this effect prior to the release of data by a registry.

Publication of data on a website and in unrestricted circulations of reports or documents containing data should be regarded as being in the public domain.

4.3. Conditions for the release of identifiable data for research

The release of identifiable data for research purposes shall normally be subject to the following conditions:

- The researcher shall have the consent of the individual patients or approval from the Patient Information Advisory Group (PIAG).
- Approval shall be obtained from the relevant Multi-Centre Research Ethics Committee (MREC) or Local Research Ethics Committee (LREC).
- Copies of MREC, LREC or PIAG approval letters or equivalent bodies in local countries should be provided to NeSC.
- Consent of the clinical practitioner responsible for the patient shall be obtained. Where consultant permission cannot be sought – e.g. consultant unknown – the GP's permission shall be sought.
- A registered medical practitioner or health professional shall take responsibility for the security and use of the data;

In addition the requester shall:

- Agree in writing to observe the same principles of confidentiality as a registered medical practitioner or health professional and shall take responsibility for the security and use of the data.
- Agree to use the data only for the purpose outlined in the request.
- Not contact the registered person except where written authorisation is received by the treating clinician and Ethics Committee approval has been given.
- Ensure that publication of results will not enable any individual to be identified.
- Return or appropriately destroy all data once no longer required.
- Give due acknowledgement to the registry for provision of the data.

4.4. Release of aggregated data

Aggregated data is released to requestors provided that a written request is submitted and that there is no possibility of indirectly identifying an individual from the data due to small numbers.

4.5. Transmission of information

4.5.1. Use of telephone and fax

No individual identifiable data shall be issued over the telephone or via facsimile.

4.5.2. Post and courier services
All data issued (paper, disk or other electronic methods) shall have an accompanying letter sent, quoting the number of pages or records in the report or on the disk and must be clearly marked "Private & Confidential" and sent to a named person. Paper copies shall be enclosed and sealed in double envelopes, with the internal envelope marked confidential.

4.5.3. Electronic transmission
Confidential information shall be transmitted by a secure method. Confidential information shall be encrypted prior to transmission over the Internet or NHSNet.

If the data are encrypted and password protected, a separate letter or email shall be sent asking the recipient to telephone the NeSC for the password.

4.6. Recording of Patient Identifiable Information Requests
All completed patient identifiable information requests concerning genetic counselling shall be held in a locked cabinet under the responsibility of the Registry Manager. Electronic copies of summary replies shall be stored on a secure folder on the internal network accessible by the Registry Manager (**Mr Jipu Jiang**) and the QA Officer (**Prof Sinnott**).

Requests for patient identifiable information which are not related to genetic counselling will be kept in a locked filing cabinet accessible by the Information Team. Electronic copies will be kept in a secure folder on the NeSC internal network accessible by the Information Team.

5. Responsibilities
Access to patient identifiable information held electronically or in paper format is controlled; staff and managers have appropriate designated levels of access to electronic information, and working practices and physical security restrict access to paper records to a 'need to know basis'. There will be an annual update related to confidentiality given to all staff.

5.1. Management responsibilities
Managers shall ensure that:
1. staff are aware of this policy and understand their responsibilities under it.
2. staff are following the policy.
3. any adverse incidents are reported to the NeSC Director or a member of the senior management team.

5.2. Staff responsibilities
Staff shall ensure that:
1. they make themselves aware of the policy and follow it.
2. they never examine or handle in any way personal data, except in the course of their work. If they are required to read personal data as part of their work, this data shall never be disclosed to any person not directly concerned with that work.
3. the data they are working on are not read or handled by anyone who has no reason to do so.
4. if they believe that someone is deliberately attempting to read or handle personal data not within their official duties, the facts must be reported immediately to their manager, or the NeSC Director or a member of the senior management team.
5. if they are working with personal data and they have to leave the room they must either lock the data away or ask another member to be responsible for the data until they return.
6. if they are the only member left in charge of personal data and they have to leave, the data must be locked away, the room locked and the windows closed.

7. confidential information is never left unlocked in an unattended room; it must be kept in secure locked cupboards or cabinets or in a secure filing room when not in use, and must not be taken out of the NeSC premises except for specified purposes authorised by the NeSC Director.
8. if it is ever discovered or even suspected that confidential information has been lost, their manager must be informed immediately; he/she shall investigate and report to the NeSC Director without delay.
9. keys to cupboards holding confidential information are locked away or kept on the person when not in use.
10. they always "log out" of their PCs when leaving the building or leaving the office empty, and 'lock' their PC screen using Alt&Control&Delete when leaving their desk/ office.
11. visitors to the NeSC are accompanied at all times.
12. person identifiable data is never left visible on an unattended terminal/PC screen.

6. References

- Data Protection Act (1998)
- Caldicott Committee Report (1997)
- Health and Social Care Reform Act (2001)
- The Health Service (Control of Patient Information) Regulations 2002
- Health and Social Care Act 2001 (www.hmso.gov.uk/acts/acts2001/20010015.htm)
- Statutory Instrument 2002 No. 1438. The Health Service (Control of Patient Information) Regulations 2002 (www.legislation.hmso.gov.uk/si/si2002/20021438.htm)
- Guidance notes. Section 60 of the Health and Social Care Act 2001 (www.advisorybodies.doh.gov.uk/piag/s60guidancenotes.PDF)
- Use and disclosure of health data. Guidance on the application of the data protection act 1998. May 2002. Information Commissioner. (www.dataprotection.gov.uk)

Confidentiality Agreement

National E-Science Centre (NeSC)

Confidentiality Undertaking for NeSC Staff

I, the undersigned, understand that, in the course of my work, I may come into contact with, or have access to, a wide range of confidential data relating to individual patients, various members of staff, confidential reports and other sensitive information.

I understand that misuse of this information, especially its disclosure to people or agencies who are not authorised to receive it, would constitute a serious breach of confidentiality. Any breach of confidence will lead to disciplinary action, which may involve dismissal. I also understand that the use and security of personal information is subject to the provisions of the Data Protection Act 1998 and that unauthorised disclosure of personal information is an offence under the Act.

I confirm that I have been made aware of the of NeSC Confidentiality policy which deals with the handling of confidential information in the NeSC, and the Information Security Policy, which is concerned with rules and procedures governing access to cancer data, and that I have read and understood the requirements of the document.

Signed . .....

Name .....

Date .....

Witnessed .....

PLEASE RETURN THIS DOCUMENT WHEN SIGNED TO THE PROF SINNOTT