



Cancer Screening Programmes

NHS Cancer Screening Programmes

Confidentiality and Disclosure Policy

VERSION 3

JULY 2009

NHS CANCER SCREENING PROGRAMMES

CONFIDENTIALITY AND DISCLOSURE POLICY

1 Introduction and Scope

This document defines the Confidentiality and Disclosure Policy for the NHS Cancer Screening Programmes in England and covers all information (in all its forms), information systems, environment and relevant people who support the programme. This document sets out the programme's policy for the protection of identifiable patient information (especially with regard to confidentiality, integrity and availability).

The NHS Cancer Screening Programmes in England place a very high importance on the confidentiality of information maintained and processed on behalf of the NHS and patients. It is the responsibility of all staff involved in the programmes to comply with this policy as a minimum standard, together with any supporting policies local to the host Trust or Authority, procedures and other relevant legislation. **Failure to comply may result in disciplinary procedures being instigated by the host employer.**

This policy will be subject to annual review by the member of staff at their individual annual appraisal.

Any work sub-contracted to the private sector must be subject to this policy. Evidence of compliance (signed proforma accepting the policy as in the appendix) must be produced before entering into a contract. (see Para 4.4 below)

2 Purpose for which data are required

- to invite people for screening and record the outcome of the invitation, using the information held on National Health Applications & Infrastructure Services (NHAIS)
- to undertake audits of the screening process
- to evaluate the Programmes' outcomes which may require data from a number of sources including the patient's GP
- to use inter-Trust and intra-Trust transfer of data in order:

- to identify the outcome of the referral from screening
- to ascertain screening history and material in order to provide the patient with information about review of past screening management
- to carry out failsafe activities
- to trace people, by the use of NHAIS Open Exeter, who may need to be contacted in the event of screening incidents and in order to provide failsafe
- to send to and receive data with the Cancer Registries in order to validate completeness of records within the Cancer Registries and the NHS Cancer Screening Programmes
- to undertake quality assurance and education
- to allow external quality assurance of local screening services' activities.

Every effort should be made to use anonymised rather than identifiable data. Where identifiable data must be used, then they should be pseudonymised wherever possible.

3 Compliance with relevant legislation and guidance

The NHS Cancer Screening Programmes Confidentiality and Disclosure Policy is based on the recommendations made in the following legislation and publications:-

3.1 The Caldicott Committee: Report on the Review of Identifiable Patient Information Dec 1997

These guidelines cover issues surrounding identifiable patient information and specify the need for a Caldicott Guardian to be appointed in all organisations using this type of information. Local services must know the name of their local Caldicott Guardian. A full list of NHS Caldicott Guardians is available from IPU (Information Policy Unit), Department of Health, Quarry House, Leeds, or on their web-site (www.doh.gov.uk/ipu/confiden/guard)

Under the guidelines, training must be provided for all staff on an annual basis in NHS Trusts/PCTs by the Caldicott Guardian or his/her nominated representative. Caldicott Guardians should confirm that all staff have been trained in such a way that QA teams can check compliance at QA visits.

The Caldicott guidelines also give details of the audit of the confidentiality and security procedures that should be carried out on an annual basis.

3.2 Data Protection Act 1998

The Data Protection Act 1998 applies only to living individuals and requires:

- a named lead to manage data protection compliance must be identified by each service, who will work with the Caldicott Guardian for local Trust/Authority/PCT
- internal training, current awareness and updates should be carried out by the host Trusts/PCTs.

These should be recorded in such a way that QA teams can check compliance at QA visits.

These functions may be fulfilled by the same individual who performs Caldicott guidelines duties. A full list of data protection registrations is available from their web-site www.dpr.gov.uk.

Details of all confidential databases will be given to the local Lead for Data Protection Compliance who will maintain a database of this information.

3.3 Health and Social Care Act 2001 – Section 60

The Health and Social Care Act 2001 brings the issue of informed consent to the fore. It states that to hold and use any identifiable patient data needs the specific informed consent of each patient.

There are exemptions covering data that are needed for the public interest and specific cases can be taken to the Secretary of State under Section 60. The legislation is likely to lead “to the use of more anonymised and pseudonymised data sets”.

Section 60 of the Health and Social Care Act 2001 enables the Secretary of State to make Regulations for and in connection with requiring or regulating the processing of patient information in prescribed circumstances.

The Act:

- allows for identifiable patient information to be processed without informed consent in support of prescribed activities, such as cancer registration, subject to Regulations which must be agreed by Parliament
- requires that consistent use of informed consent should be the usual basis for handling identifiable patient information
- states that Regulation can provide for processing of identifiable patient information for medical purposes where there is benefit to patient care or in the public interest
- states that Regulation can only allow processing of information where there is no reasonable alternative
- requires the Secretary of State to consult with interest groups and also the Patient Information Advisory Group (PIAG) established in December 2001.
- Will require the affirmation of both Houses of Parliament
- States that identifiable patient information remains covered by the Data Protection Act 1998, and common law as established in case law.

The NHS Cancer Screening Programmes in England received PIAG support in March 2003 and will be subject to annual review.

3.4 **General Medical Council Guidance**

The GMC booklet “Confidentiality: Protecting and Providing Information -

Section 1 - Patients’ right to confidentiality” places responsibilities upon doctors to:

- “seek patient’s consent to the disclosure of information wherever possible, whether or not the doctor judges that patients can be identified from the disclosure
- anonymise data where unidentifiable data will serve the purpose and
- keep disclosures to the minimum necessary.

The doctor must be prepared to justify their decisions in accordance with this guidance.”

The duty of confidentiality continues after death. Section 5 - paragraph 40 - Disclosure after a patient’s death states that “the extent to which confidential information may be disclosed after a patient’s death will depend on the circumstances. These include the nature of the information, whether the information is already public knowledge or can be anonymised, and the intended use to which the information will be put. The doctor should also consider whether the disclosure of the information may cause distress to, or be of benefit to, the patient’s partner or family.”

3.5 **British Standard BS7799 (1995/1999)**

This is a British Standard relating to security issues around use of IT in all areas of business. It is being adopted by the NHS and promoted by the NHS Information Authority. The NHS Cancer Screening Programmes seeks to achieve compliance with this standard as soon as possible. Local Cancer Screening Programmes must be aware of the areas it covers and consider them in its Security, Confidentiality and Disclosure procedures and policies. Compliance should be recorded in such a way that QA teams can check at QA visits.

4 Identifiable Patient Information

4.1 Requests to the NHS Cancer Screening Programmes for non-routine identifiable patient information

In order for the request to be considered and approved, a case must:

- show why identifiable patient data are required and why anonymised or pseudonymised data cannot be used
- provide details on how the data will be kept and confirmation that they will be destroyed after use.

All transfer of identifiable information other than for patient care purposes or to Cancer Registries and other organisations covered by the NHS Cancer Screening Programmes PIAG application, must be covered by a separate PIAG approval obtained by the organisation requesting the data.

Data cannot be used for a different purpose from that for which they were collected ie. screening of women and audit, monitoring and evaluation of the screening programme.

Staff must direct all requests for non-routine information to the local programme lead and must not at any time disclose or release information of any nature unless specifically authorised to do so by the programme lead in the trust. This will be Directors of breast screening, the Director for colorectal screening, lead pathologists, lead colposcopists or hospital-based co-ordinators for cervical screening and the screening commissioners for the appropriate PCTs for the recall system and acceptance data. In considering requests for access, the local programme lead in the trust will ensure that disclosure is of the minimum data required to meet the purpose and that wherever possible only anonymised data are disclosed.

All requests for information and any resulting action must be recorded together with the disclosure/resulting action. Policies should be checked for compliance at QA visits.

4.2 **Disclosure of Information**

Local written policies must be in place to identify responsibilities for dealing with routine requests for data which complies with national guidance.

Disclosure to patient or carer or next of kin (including after death)

Access to health records of deceased people is governed by the Access to Health Records Act 1990. Under this Act, when a patient has died, their personal representative, executor, administrator, or anyone having a claim resulting from the death (this could be a relative or any other person) has the right to apply for access to copies of the deceased's health records.

4.3 **Storage of Identifiable Patient Information by the NHS Cancer Screening Programmes**

Where possible, all electronic data should be stored on a network server. Not all staff have access to a network server and data are held on the hard disk drive of PC's and on a temporary basis on laptops, to service a particular clinic.

When the data are stored on a local hard disk or on magnetic media (e.g. floppy disk, CD) it is the responsibility of the user to ensure that they are password protected and removed or destroyed as soon as possible.

Details of the specific circumstances and procedures, when identifiable patient data may be used off site, must be described in Standard Operating Procedures and approved by the Caldicott Guardian.

All paper records of confidential information will be stored in a secure location.

The data should be protected from unauthorised access in all eventualities.

Data should be anonymised as soon as possible when using it for analysis.

4.4 External Contractors

Written contracts must be set up and signed with all persons or organisations who have access to confidential data held by the NHSIA or NHS Cancer Screening Programmes.

All such contractors must agree to comply with the requirements of this policy. In particular, checks must ensure that this policy's requirements will cover off-site filing, the use of couriers, bulk postage and digitising information onto PCs.

This requirement covers processing of both electronic and paper records.

4.5 Disposal of Confidential Information

Data in whatever format which are no longer required must be disposed of in a permanently irretrievable form.

Confidential paper records must not be disposed of in readable form. There must be secure arrangements for disposal.

All screening materials should be destroyed by an appropriate secure method as agreed by local policies.

Guidance on retention of screening materials is detailed in the NHSBSP Good Practice Guide no.5 Jan 2001 and the BSCC Recommended Code of Practice for Laboratories Providing a Cytopathology Service 1997.

Paper used for scrap must not include any personal data.

Retention of electronic data on previously screened women is expected in order to facilitate audit and in anticipation of requests for screening by women beyond invitation age.

5 General Issues

Tables, reports or graphs derived from data held, should be displayed so as to minimise the risk of identification because of the level of detail appearing in routine reports. Attention should be paid to the size of the numerator and the denominator.

Any demonstrations of the databases should take place using fictitious data.

Written policies should be in place to deal with transmissions of information which should be restricted as follows:

- Mail – use of plain envelopes is recommended (do not use transit envelopes). All outgoing paper records will be marked private and confidential and (if very heavy) double wrapped or sent by recorded delivery
- All electronic-transmission of identifiable data to be sent separately from other information. Access to data transmitted by magnetic medium to be accessed by means of a password which should be issued separately, or via telephone once data are received
- E-mail – identifiable patient data must not be sent via e-mail unless this is via an encrypted e-mail sent on the NHS net and password protected
- Fax - must be secure in a 'safe haven ' area, with immediate collection and receipt confirmed
- Telephone – no identifiable patient information will be given to an unrecognised or an unverified person over the telephone. All requests for information taken over the telephone must be recorded and logged for internal requests and must be in writing for external requests. Always call the person back to check identity before releasing identifiable patient information over the telephone
- Transport - robust mechanisms for receipt and dispatch of materials sent out for reporting are required.

6 Validity of this Policy

This policy is effective immediately and will be reviewed annually under the authority of the Programme's National Coordination Team, before PIAG review submission.

GLOSSARY OF TERMS

The following terms are used in the definitions:

Anonymised data - has had all identification removed from the data and cannot be tracked back.

Pseudonymised data - is where the data has been given a different identification from the original and the patient can be identified from the original list using a code/key.

Failsafe - a system to ensure that people are not lost to the screening programmes

DEFINITIONS

Patient Information – any information that is, or is derived from, information concerning a patient's physical or mental health or condition, the diagnosis of their condition or their care or treatment. In addition to information which directly identifies individuals, this would include information which is either anonymised (e.g. any information that cannot be tracked back to the individual) or coded (e.g. information that can be tracked back to an individual by persons in possession of the key to the code). It includes information recorded in any manner, whether electronically or manually.

Identifiable patient information (also referred to as confidential patient information) – is defined as:

- personal details of any patient or carer (e.g. name, address, postcode, telephone number, date of birth) and hospital numbers or other unique identifiers of any health service patient, including the NHS number
- any information pertaining to diagnosis, prognosis or treatment of patients where this is linked to details that may enable the person to be personally identified

Patient Information (as defined in the Health & Social Care Act 2001)

“For the purposes of this section, patient information is “confidential patient information” where:

- (a) the identity of the individual in question is ascertainable:
 - (i) from that information, or
 - (ii) from that information and other information which is in possession of, or is likely to come into the possession of the person processing that information, and

- (b) that information was obtained or generated by a person, who, in the circumstances, owed an obligation of confidence to that individual.

Personal data – (as defined in the Health & Social Care Act 2001)

data consisting or information which relates to a living individual who can be identified from that information (or from that and other information in the possession of the data controller or which is likely to come into the possession of the data controller.).

Processing -(as defined in the Health & Social Care Act 2001)

this includes obtaining and the retention of data as well as manipulation and analysis

Data Protection Principles

The Act states the following are principles:

- 1 Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:
 - at least one of the conditions in Schedule 2 of the Data Protection Act 1998 is met, and
 - in the case of sensitive personal data, at least one of the conditions in Schedule 3 of the Data Protection Act 1998 is also met.

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. Note:

- all purposes are specified and lawful and cover the processing
- disclosure must be compatible with purposes for which data were obtained.

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

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

Note:

- reasonable steps must be taken to ensure accuracy
- provision must be made for subject's comments in relation to the accuracy of data pertaining to them.

5 Personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose or those purposes

Note:

- procedures for retention and disposal of records are included in this policy.

6 Personal data shall be processed in accordance with the right of data subjects under this Act.

Note:

- procedures satisfy rights of data subjects.

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.

Note:

- best practice on information and IT security is covered in this policy
- there is capability to respond to a breakdown in operations
- written contracts are established with all data processors undertaking work for the local host Trust/Authority.

8 Personal data shall not be transferred to a country or territory outside the European Union, 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.

Data Subject – individuals to whom personal data relates.

Data user – person(s) or organisation(s) who controls the contents and use of a collection of personal data (processed, or intended to be processed, automatically).

Disclosure – a disclosure occurs whenever the data of information extracted from the data held are passed (in any format) to someone other than the data user.

Disclosure of Personal Data – occurs when data identifies the data subject or can be used to identify the data subject to whom they relate.

Fair and lawful processing – means that:

- the common law of confidentiality is complied with
- persons were not misled, deceived or coerced into giving data
- basic information on users and uses of the data are given
- for health data, the conditions in Schedule 3 of the data Protection Act 1998 are applied
- data sharing protocols in response to Caldicott guidelines must also comply with Data Protection Act 1998

- data subjects should usually be informed about the identity of the data controller and uses of the data.

Defined in the Health & Social Care Act 2001 as

“For the purposes of this section, patient information is “confidential patient information” where:

(a) the identity of the individual in question is ascertainable:

(i) from that information, or

(ii) from that information and other information which is in possession of, or is likely to come into the possession of the person processing that information, and

(b) that information was obtained or generated by a person, who, in the circumstances, owed an obligation of confidence to that individual.

Personal data – data consisting or information which relates to a living individual who can be identified from that information (or from that and other information in the possession of the data controller or which is likely to come into the possession of the data controller).

Processing - this includes obtaining and the retention of data as well as manipulation and analysis.

**DECLARATION OF COMPLIANCE WITH CONFIDENTIALITY AND DISCLOSURE
POLICY
(FOR STAFF, PRIVATE SECTOR EMPLOYEES/SUB-CONTRACTORS)**

I understand that in the course of my work, I may come into contact with, or have access to, confidential information relating to individual patients or NHS staff. 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.

I have read and understood the NHS Cancer Screening Programmes Confidentiality and Disclosure Policy. I understand that failure to adhere to the policy may lead to disciplinary action. I also understand that intentional divulgence of identifiable patient information in breach of this policy 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 a criminal offence under the Act.

Name:Title:

Signed:Date: