



Cancer Screening Programmes

NHS Cancer Screening Programmes

Confidentiality and disclosure policy

Version 4: August 2011

Version control sheet

Confidentiality and disclosure policy	
Version	4
Status	Final
Author/ originator	Phil McCorry/ Anny Jones
Responsible Director	Phil McCorry
Approved by	Julietta Patnick
Date issued	31 August 2011
Last review date	N/A
Next review date	31 August 2012
Applies to	All staff, contractors and volunteers employed in NHS Cancer Screening Programmes

Version	Description of change	Reason for change	Author	Date
4	New section plus general updating	Inclusion of information on potentially identifiable patient data	Phil McCorry/ Anny Jones	September 2010–August 2011

CONTENTS

1. INTRODUCTION AND SCOPE	4
1.1 The purpose and scope of this policy	4
1.2 The duty of confidentiality	4
1.3 Compliance with this policy	5
2. PURPOSE FOR WHICH PATIENT DATA ARE REQUIRED	6
3. COMPLIANCE WITH RELEVANT LEGISLATION AND GUIDANCE	7
3.1 The Data Protection Act 1998	7
3.2 Human Rights Act 1998	7
3.3 Health and Social Care Act 2001, NHS Act 2006, Health and Social Care Act 2008	7
3.4 Administrative Law	8
3.5 Common Law of Confidentiality	8
3.6 <i>Confidentiality: The NHS Code of Practice 2003</i>	8
3.7 <i>NHS Records Management: Code of Practice 2006</i>	8
3.8 <i>Information Security Management: NHS Code of Practice 2007</i>	9
3.9 <i>British Society for Clinical Cytology: Recommended Code of Practice for Laboratories Participating in the UK Cervical Screening Programmes 2010</i>	9
3.10 <i>The Caldicott Committee: Report on the Review of Identifiable Patient Information December 1997</i>	9
3.11 <i>General Medical Council (GMC) Confidentiality Guidance October 2009</i>	9
3.12 <i>Office for National Statistics Health and Care 2006. Review of the Dissemination of Health Statistics: Confidentiality Guidance</i>	10
3.13 <i>United Kingdom Association of Cancer Registries Guidelines on release of: a) individual level anonymised information and b) tabular information based on small populations or small cell counts (potentially identifiable information)</i>	10
3.14 <i>ISO/IEC 27001–27006</i>	10
4. DISCLOSURE OF IDENTIFIABLE PATIENT INFORMATION (IPI)	12
4.1 Definition	12
4.2 Disclosure of identifiable patient information	12
4.3 Consent to disclosure	12
4.4 Disclosure of information relating to individual patient healthcare	12
4.5 Disclosure of information NOT relating to individual patient healthcare	13
4.6 Disclosure of IPI relating to deceased patients	15
4.7 Storage of IPI by NHS Cancer Screening Programmes	15
4.8 External contractors and charitable organisations	15
4.9 Disposal of confidential information	16
5. POTENTIALLY IDENTIFIABLE PATIENT INFORMATION (PIPI)	17
5.1 Definition	17
5.2 Disclosing PIPI	17
5.3 Approval to disclose PIPI	18
5.4 Documenting the disclosure of PIPI	18
5.5 Geographical patient information that is potentially identifiable	18
5.6 Minimising risk with PIPI	19
6. GENERAL ISSUES	21
6.1 Keeping patient information secure	21
6.2 Transferring records	21
7. VALIDITY OF THIS POLICY	23
GLOSSARY	24
APPENDIX 1 DECLARATION OF COMPLIANCE (COPY 1)	27
APPENDIX 1 DECLARATION OF COMPLIANCE (COPY 2)	28
APPENDIX 2 KEEPING PATIENT INFORMATION SECURE	29

NHS CANCER SCREENING PROGRAMMES CONFIDENTIALITY AND DISCLOSURE POLICY

1. Introduction and scope

1.1 The purpose and scope of this policy

NHS Cancer Screening Programmes (NHS CSP) in England are committed to creating, maintaining and managing the security of their key information assets and of the external information resources on which these assets depend. This policy sets out principles and procedures for safeguarding the confidentiality and disclosure of patient information that is actually or potentially identifiable. In doing so it acknowledges that most NHS records, including staff and administrative records, contain sensitive or confidential information. The processing of patient data, but also of data relating eg to complaint handling, personnel, financial or occupational health matters, is regulated by *The Data Protection Act 1998*, the common law duty of confidentiality and *the Human Rights Act 1998*, and must comply with them.

The confidentiality of identifiable or potentially identifiable information relating to staff or to patients should at all times be duly safeguarded. This policy focuses primarily on patient data: on their confidentiality, integrity, protection, use and disclosure. For the purposes of this document the term 'patient' covers all individuals whose data are stored or processed by or on behalf of NHS CSP, whether or not they are or become the subject of active care or treatment.

This policy covers all information processed (whether in print, digital or other form), as well as the information systems and wider information environment that support it. It applies to all staff and contractors employed in or by NHS CSP, including the NHS Breast Screening Programme (NHSBSP), NHS Cervical Screening Programme (NHSCSP), and NHS Bowel Cancer Screening Programme (NHS BCSP) but excluding General Practices, which are covered by the local implementation of national Information Governance protocols.

1.2 The duty of confidentiality

The NHS CSP place a very high importance on the confidentiality of information maintained and processed on behalf of their patients and the NHS. *Confidentiality: NHS Code of Practice (2003)* states that a duty of confidence arises when one person discloses information to another in circumstances where it is reasonable to expect that the information will be held in confidence. It is a legal obligation and a professional requirement to hold such information in confidence. In the NHS this obligation must be

included in employment contracts, linked to disciplinary procedures and embedded in organisational systems and processes.

It is the responsibility of all staff, contractors and volunteers working in NHS CSP to comply with this policy as a minimum standard, together with any supporting policies or procedures local to the host organisation (eg NHS Foundation Trust) and other legal obligations. Failure to do so may result in disciplinary procedures being instigated by the host employer and personal liability. If they are unsure how to handle patient-identifiable information they should contact the relevant information governance lead or Caldicott Guardian. (See 3.3) In the interests of good practice, employers should ensure that staff receive, as a minimum, a three-yearly update on the specific issues surrounding the confidentiality and disclosure of patient data for screening. (This is in addition to the information governance training tool assessment that must be completed annually by NHS staff.)

1.3 Compliance with this policy

Bodies whose staff will or may gain access to (actually or potentially) identifiable patient information while providing services to the NHS CSP are required formally to declare compliance with this policy. Among these bodies are units directly engaged in providing screening services and organisations providing such services within one or more Trusts. In each case, a named lead at Board level (eg the Caldicott Guardian or Senior Information Risk Owner) should be identified by each service within a programme to declare compliance across that programme using the form at Appendix 1. This form must be signed and produced before the start of any contract that will or may involve access to (actually or potentially) identifiable patient information, and compliance must cover the life of that contract.

In the interests of good practice, it is recommended that compliance with this policy is checked annually at individual staff appraisals.

2. Purpose for which patient data are required

NHS CSP use patient data

- to invite people for screening and to record the outcome of the invitation, using information held on the National Health Applications and Infrastructure Services (NHAIS) system
- to undertake audits of the screening process
- to evaluate NHS CSP outcomes, which may require data from a number of sources including the patient's GP
- for the inter-Trust and intra-Trust transfer of data
 - to identify the outcome of the referral from screening
 - to assemble a screening history and related material in order to provide the patient with information on past screening management
 - to carry out failsafe activities
- from the NHAIS system, to trace people who may need to be contacted (a) in the event of screening incidents and (b) to provide failsafe
- to send data to and receive them from cancer registries in order to validate the completeness of the registries' records and those of NHS CSP
- to undertake quality assurance, training and education
- to allow external quality assurance (QA) of local screening service activities.

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

3. Compliance with relevant legislation and guidance

The disclosure and use of confidential patient information must be lawful and ethical. A named lead should be identified by each service to work with the host Trust's Caldicott Guardian (see 3.3), Information Governance Manager, Senior Information Risk Owners and Information Asset Owners as appropriate on managing data protection compliance. This compliance should be supported by internal training, current awareness audits and updates; it should be monitored locally and formally recorded for QA purposes. Details of all confidential databases must be supplied to the local lead for data protection compliance, who maintains a register of such information.

The principles and provisions enshrined in this policy are derived from the following legislation and publications.

3.1 **The Data Protection Act 1998**

(http://www.ico.gov.uk/what_we_cover/data_protection.aspx)

This Act governs the processing of personal data. It prohibits information processing unless specific conditions are met. (These are set out in Schedules 2 and 3 of the Act and include consent conditions.) It identifies eight principles that underpin standards for information handling; the most significant of these are that

- processing must be fair, lawful and in accordance with the rights of the data subject
- personal data must be processed for one or more specified and lawful purposes and not processed further for incompatible purposes
- personal data must be protected against unauthorised or unlawful processing and against accidental loss, destruction or damage.

3.2 **Human Rights Act 1998**

(<http://www.opsi.gov.uk>)

Article 8 of this Act establishes a duty to protect the privacy of individuals and preserve the confidentiality of their health records. Actions that interfere with the right to respect for private and family life (eg disclosing confidential information) must be necessary to support legitimate aims which are set out in statute and must be proportionate to the need.

The 'necessity test' is also fundamental to the duty of confidence and the Data Protection Act, making their aims impossible to achieve without it. It therefore represents a higher threshold than convenience.

3.3 **Health and Social Care Act 2001, NHS Act 2006, Health and Social Care Act 2008**

(<http://www.nigb.nhs.uk/>)

In 2001 the *Health & Social Care Act* acknowledged the need to seek patients' explicit consent before their details were passed from agency to agency. In cases (such as NHS CSP) where it was impractical to obtain this consent from patients, exemption could be sought from the Patient Information Advisory Group (PIAG) under Section 60 of the Act.

Under the *NHS Act 2006*, Section 60 was re-enacted by Section 251, permitting the Secretary of State for Health to allow the duty of confidentiality to be set aside in medical contexts where using anonymised information is not possible and seeking individual consent is impracticable.

The *Health and Social Care Act 2008* established the National Information Governance Board for Health and Social Care (NIGB) to provide a single authoritative source on information governance issues where there was disagreement about best practice. In 2009, the NIGB's Ethics and Confidentiality Committee (ECC) replaced the PIAG, to become responsible for administering all Section 251 applications to set aside confidentiality in specific cases.* Section 251 requires that approval is considered only where consent is genuinely impracticable and where pseudonymised or anonymised data will not suffice. This new arrangement enables identifiable patient information to be disclosed and used without patient consent for essential NHS activity and medical research where it is in the public interest to do so.

Although Section 251 permits the common law of confidentiality to be set aside, it does not override obligations under the Data Protection Act 1998.

3.4 **Administrative Law**

This states that a public authority must possess the power to carry out what it intends to do. It also requires this power to be exercised for the purpose for which it was created or be 'reasonably incidental' to the defined purpose.

3.5 **Common Law of Confidentiality**

Although not written in statute, this body of law makes clear that information given in confidence should not, except in exceptional circumstances, be used or disclosed further without the confider's permission.

3.6 **Confidentiality: The NHS Code of Practice 2003**

(<http://www.dh.gov.uk>, where periodic updates can also be found)

This key document introduces the concepts of confidentiality and disclosure, outlines the principal legal and other requirements for a confidential service, and provides a decision-making tool for sharing or disclosing information, along with sample contexts for its use.

3.7 **NHS Records Management: Code of Practice 2006**

* These arrangements are current at the time of writing but may be subject to change as part of the NHS reorganisation.

(www.dh.gov.uk)

This sets out standards of practice for all aspects of NHS records management, from creation to disposal. It is based on current legal requirements and professional good practice and applies to all patient and administrative records, whatever their form.

3.8 ***Information Security Management: NHS Code of Practice 2007***
(<http://www.dh.gov.uk>, where periodic updates can also be found)

This guide to the methods and standards of practice in information security management is based on current legal requirements, relevant standards and professional best practice. It is a key component of information governance arrangements for the NHS and its guidelines apply to NHS information assets of all types.

3.9 ***British Society for Clinical Cytology: Recommended Code of Practice for Laboratories Participating in the UK Cervical Screening Programmes 2010***
<http://www.clinicalcytology.co.uk/resources/resources.asp>

The guidance gives laboratories within the UK's cervical screening programmes examples of good practice across a range of areas, among them the disposal of confidential information.

3.10 ***The Caldicott Committee: Report on the Review of Identifiable Patient Information December 1997***
(<http://www.dh.gov.uk>)

The report covers questions relating to identifiable patient information, including guidance on auditing confidentiality and security procedures. It sets out six key principles designed to ensure that patient-identifiable information is not disclosed inappropriately

- justify the purpose(s)
- don't use patient identifiable information unless it is absolutely necessary
- use the minimum necessary patient identifiable information
- access to patient identifiable information should be on a strict need-to-know basis
- everyone with access to patient identifiable information should be aware of their responsibilities
- understand and comply with the law

It establishes the role of the Caldicott Guardian in supporting lawful and ethical processing and (where appropriate) sharing of patient identifiable information within and between organisations.

3.11 ***General Medical Council (GMC) Confidentiality Guidance October 2009***
(<http://www.gmc-uk.org/guidance/>)

This sets out the GMC's confidentiality principles, among them that

- notwithstanding the doctor's duty of confidentiality, appropriate information sharing is essential to the efficient provision of safe, effective care
- doctors should ensure patient awareness of the circumstances in which personal information may be disclosed
- doctors should confirm (a) that patients know they can object to this disclosure and (b) that they have not done so
- doctors must obtain express patient consent if identifiable information is to be disclosed for purposes other than their care or local clinical audit, unless the disclosure is required by law or can be justified in the public interest
- anonymised or coded information must be used if practicable and if it will serve the purpose
- disclosures must be kept to the minimum necessary and observe all relevant legal requirements
- when satisfied that specific information should be disclosed, doctors should act promptly to disclose it
- patients' legal rights to (a) be informed about how their information will be used and (b) have access to, or copies of, their health records should be respected and supported.

3.12 **Office for National Statistics *Health and Care 2006. Review of the Dissemination of Health Statistics: Confidentiality Guidance***

(<http://www.ons.gov.uk/about/consultations/closed-consultations/disclosure-review-for-health-statistics---consultation-on-guidance/consultation-summary.pdf>)

This document proposes a general framework for protecting the confidentiality of health statistics, with an emphasis on risk assessment and management. It underlines the importance of understanding which data may need protection and provides a list of factors to take into account.

3.13 **United Kingdom Association of Cancer Registries *Guidelines on release of: a) individual level anonymised information and b) tabular information based on small populations or small cell counts (potentially identifiable information)***

(<http://82.110.76.19/confidentiality/potentiallyidpolicy.asp>)

This sets out guidelines (specifically for cancer registries but largely applicable to NHS CSP) in relation to the disclosure or publication of data that are potentially, rather than actually, identifiable.

3.14 **ISO/IEC 27001–27006**

(<http://www.iso.org/iso/catalogue/>)

ISO/IEC 27001 (2005) replaces BS7799-2:2002 as the set of specifications against which organisations may seek independent certification of their Information Security Management System (ISMS). It specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS. It is designed to ensure the selection of adequate and proportionate security controls to protect information assets. It is

supported by a code of practice (27002: 2007) and guidance on: specifying and designing information management systems (27003: 2010), developing and using measures to assess their effectiveness (27004: 2009), managing their risks (27005:2011), and audit and certification (27006: 2011).

4. Disclosure of identifiable patient information (IPI)

4.1 Definition

IPI is individual information that is either clearly identifiable or at very high risk of being identified because the identity of the individual is ascertainable

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

It includes

- (i) the personal details of a patient or carer (eg name, date of birth, address, full postcode, telephone number, separately or in combination) or the unique identifier of any health service patient, including the NHS number
- (ii) any information pertaining to the diagnosis, prognosis or treatment of an individual where this is linked to details that may enable that person to be identified

This information is *confidential* when it was obtained or generated by a person who, in the circumstances, owed a duty of confidence to that individual.

4.2 Disclosure of identifiable patient information

A patient's health records are made by the health service to support that patient's healthcare. Information that can identify individual patients must be processed in accordance with the Data Protection Act 1998, the common law duty of confidentiality and the Human Rights Act. It must be kept private and physically secure. It must not be used or disclosed for purposes other than healthcare without the individual's explicit consent or where there is a clear public interest or legal justification for doing so.

4.3 Consent to disclosure

Patients must be made aware of information disclosures that are necessary to provide them with high quality care. These disclosures may be in the course of clinical governance and clinical audits, or where information is shared between members of care teams and between different healthcare (including non-NHS) organisations. IPI provided in confidence should not be used or disclosed in a form that might identify a patient without his or her consent. The exceptions to this rule are where there are statutory grounds for disclosing it; some of these grounds are listed in *Confidentiality: NHS Code of Practice Annex C*.

4.4 Disclosure of information relating to individual patient healthcare

Patients generally have the right to object to the use or disclosure of confidential information that identifies them, and should be made aware of this right. However if a patient objects it might, in exceptional cases, limit the care or treatment options available. Patients must be informed if their decision about disclosure has implications for their care or treatment.

Provided patients have been informed of

- (a) how information relating to their healthcare will be used and disclosed
- (b) the choices they have in relation to that use and disclosure
- (b) the implications of opting to limit how that information may be used or shared

their explicit consent is not usually required for the IPI disclosures needed to provide their healthcare, as consent is taken to be implied in their agreement to examination and treatment. Opportunities should nevertheless be taken to check that patients understand what may happen and are content.

4.5 **Disclosure of information NOT relating to individual patient healthcare**

Consent cannot be assumed in cases where the purpose of the disclosure is not directly concerned with individual patient healthcare. Either additional efforts to gain consent are required or alternative approaches that do not rely on identifiable information need to be developed. It should be borne in mind that patients have different needs and values: an issue that does not appear sensitive may be important to an individual patient in those particular circumstances.

4.5.1 **Routine use of patient identifiable information**

There are some routine NHS CSP activities (eg clinical audit, release of data to cancer registries or call/ recall) for which obtaining individual consent to the use or disclosure of IPI is impracticable, yet where the public benefit of disclosure would generally outweigh issues of privacy. In these cases, Section 251 of *The Health and Social Care Act 2008* permits health or social care bodies to apply to the NIGB's Ethics and Confidentiality Committee (ECC) for the duty of confidentiality to be set aside, allowing IPI to be used without individual consent. (See Section 3.7.) Where a patient formally objects to disclosure, however, this should normally be respected

4.5.2 **Non-routine use of patient identifiable information**

Within NHS CSP, most transfers of IPI are for patient care purposes or to organisations covered by NHS CSP's annual application for support under the Health Service (Control of Patient Information) Regulations 2002.

In all other instances separate NIGB/ECC approval must be obtained by the organisation requesting the data.

The decision to release IPI in response to a non-routine request should be guided by a set of clear and established principles enshrined in a formal agreement. For such a request to be considered and approved, a case must be made to the NIGB/ECC

- clearly stating and explaining the intended uses of the data
- showing why identifiable patient data are required and why anonymised or pseudonymised data cannot be used

- providing details on how the data will be kept and confirmation that they will be destroyed after use.

The IPI released

- must be no more detailed or extensive than is needed to fulfil the stated purpose
- must not be used for a purpose other than that for which release was approved
- must be held securely until its stated purpose is met and then destroyed
- must not be passed on to third parties or released into the public domain

No attempt should be made to identify IPI relating to particular individuals or to contact individuals. The information should not be linked to other datasets unless this has been agreed with the data providers. If analyses of the data are to be made public in reports or papers these should be shared, before publication, with the source that supplied the information.

- **IPI for which a local screening service has responsibility:** all non-routine requests for IPI relating to the local screening population must be directed in the first instance to the local programme lead. No IPI should be disclosed or released without his or her specific authorisation. These leads are
 - *breast screening*: breast screening unit director
 - *bowel screening*: bowel screening centre director (information on patients attending screening centres); hub director (all other information)
 - *cervical screening*: hospital-based coordinators
 - *call/recall system (breast/ cervix only) and acceptance data*: the lead of the relevant call/ recall agency (this will depend on local arrangements).
- **IPI relating to a wider population:** non-routine requests to Quality Assurance Reference Centres (QARCS) to provide IPI must be directed in the first instance to the QA Director. No data should be disclosed or released without his or her specific authorisation. Data requests *from* QARCs are covered by Section 251 approval and will continue to be governed by its provisions. All other requests for IPI relating to a wider population should be directed in the first instance to NHS CSP's National Office.

All requests and any resulting action should be formally documented for QA purposes, as should disclosures and any resulting action. Related policies and procedures should be monitored for compliance.

All recipients of data under these arrangements should be familiar with this policy and should fulfil their obligations under it. (See Section 1.3.)

Any queries or concerns in relation to information requests should be raised with NHS CSP's National Office.

4.6 Disclosure of IPI relating to deceased patients

Access to the health records of deceased people is governed by the *Access to Health Records Act 1990*. Under the Act, when a patient dies their personal representative, executor, administrator, or anyone (related or not) who has a claim resulting from the death may apply to the relevant body for access to copies of the deceased's health records. Unless the patient explicitly refused such disclosure before death, these would normally be released.

4.7 Storage of IPI by NHS Cancer Screening Programmes

Identifiable patient data released for analysis should be anonymised at the earliest opportunity and protected by password and encryption against unauthorised access.

The storage of confidential records, whatever their form, should comply with the *Records Management: NHS Code of Practice*. All paper records containing IPI should be stored in a secure, lockable, location. Wherever possible, electronic data should be stored on a network server. Alternatively, consideration should be given to providing secure remote access to data. Where staff do not have such access, nor access to a network server, data may be held on an internal hard drive or C drive of a desktop or laptop computer or an external memory device (such as a USB memory stick) *only* if the disk, drive or device has been encrypted and the data have been backed up and stored in a secure location. Data should not be retained on portable devices for any longer than is absolutely necessary; it is the responsibility of users to ensure that all IPI data are removed or destroyed as soon as they are no longer needed.

Details of the specific circumstances in which IPI may be used off site and the procedures governing them must be set out in Standard Operating Procedures and approved by the Caldicott Guardian.

4.8 External contractors and charitable organisations

Bodies providing services to the NHS CSP may employ external contractor organisations (eg for off-site filing, courier services, bulk postage or digitising information for PCs). They may also use the paid or unpaid services of charitable organisations. Where staff of either type of organisation are likely to gain access, routinely or incidentally, to data held by or on behalf of NHS CSP, the responsible bodies must ensure that these individuals are contractually bound to comply with NHS data protection requirements, and must monitor their compliance. These obligations are in addition to any general written confidentiality protocols developed with the contractor or charitable body.

These requirements cover the processing of both electronic and paper records.

4.9 Disposal of confidential information

Whatever their format, data that are no longer needed must be disposed of securely, in a permanently irretrievable form, and in accordance with local policies and the *NHS Records Management: Code of Practice*. Paper records containing sensitive or personal information must not be disposed of in readable form; paper bearing personal data must not be used for scrap. Both should be shredded, as set out in *Information Security Management: NHS Code of Practice (2007)*. Further guidance is provided in the NHSBSP's *Retention, Storage and Disposal of Mammograms and Screening Records (2001)* and the BSCC's *Recommended Code of Practice for Laboratories Participating in the UK Cervical Screening Programmes (2010)*.

In accordance with NHS CSP's Section 251 approval, electronic data on previously screened people is routinely retained for audit and evaluation purposes and in anticipation of requests for screening by people beyond invitation age (eg when cancers develop in later life).

5. Potentially identifiable patient information (PIPI)

5.1 Definition

Section 4 relates to individual patient information that is either clearly identifiable or at very high risk of being identified. At the other end of the spectrum the release of highly aggregated data poses no realistic risk of individuals or their data being identified. Between these extremes lie anonymised but individual records or tabular data to a low level of aggregation. The disclosure of such information poses a very small risk of identifiability when it is combined with information either already held by the data recipient(s) or obtainable from a different source.

Particularly where the risk of disclosure concerning an individual is very small, potentially identifiable patient information should not be subject to the same regulations as actually or obviously identifiable patient information. In accordance with UK Association of Cancer Registries guidance (see 3.13), what follows is designed not to eliminate risk but to manage it.

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

- the records of individuals, even if they do not include variables (such as names, full postcodes and dates of birth) that would make them obviously identifiable
- tabular data based on small geographic areas and with low cell counts (or where low counts can be inferred by simple arithmetic) hereafter referred to as 'sparse cells'. For the majority of health statistics 'low' equates to a marginal cell total of 1 or 2 at country level. This rises to 4 or 5 where more sensitive statistics are concerned, such as those relating to sexually transmitted conditions; for smaller geographical areas, cells totalling of 5 or even 10 may be considered sparse
- tabular data containing cells that have underlying population denominators of less than approximately 1,000.

5.2 Disclosing PIPI

As with IPI, the decision to release PIPI should be guided by a set of clear and established principles that should be enshrined in a formal agreement

- the intended uses of the data should be clearly stated and justified
- the data should not be used for any other purposes
- the data released should be no more extensive or detailed than is needed to fulfil the stated purpose
- they should not be passed on to third parties or released into the public domain
- they should be held securely and once their stated purpose has been met they should be destroyed
- no attempt should be made to identify information relating to

particular individuals or to contact individuals unless patient consent has been obtained

- no attempt should be made to link the information to other datasets unless this has been agreed with the data providers
- if analyses of the data are to be made public in reports or papers these should be shared, before publication, with the source that supplied the information.

If necessary, the local programme lead should consult the Caldicott Guardian of the host organisation. Those applying for information as part of a research study may also be referred to the ECC and/or for approval by a Research Ethics Committee (REC).

It may be justifiable to release PIPI to organisations within the NHS: eg for cluster investigations, or to named researchers for specified and time-limited research projects. Research projects should be NIGB/ECC compliant and, where necessary, have REC approval (eg to include additional safeguards that the recipient will not seek to identify individuals or disclose the data to others).

5.3 **Approval to disclose PIPI**

As with obviously identifiable material, all non-routine requests for PIPI relating to the local screening population must be referred in the first instance to the local programme lead. Those relating to the wider population should be referred to National Office. (See Section 4.5.)

5.4 **Documenting the disclosure of PIPI**

All requests and any resulting action must be logged, as must the disclosure and any resulting action.

Recipients of data should be familiar with this policy and should fulfil their obligations under it. Before information is released, compliance must be declared by an authorised representative, using the form at Appendix One. (See Section 1.3.)

5.5 **Geographical patient information that is potentially identifiable**

If the total denominator population of a geographical area is 62,000 or greater, tabulations at the level of single sex, five-year age group (above 24 years), and single year of incidence are permissible.* This remains true even if they contain a proportion of cells in which the denominator is less than 1,000 and/or the numerator is less than five.

Where practical, the frequency of sparse cells should be reduced by aggregating several years of incidence, several age groups, and several diagnostic codes. Alternatively, age-standardised rates should be used.

The rarity of screen-detected cancer in children and young adults creates a significant risk of disclosure if information is published in

* For details see United Kingdom Association of Cancer Registries, *Guidelines on release of: a) individual level anonymised information and b) tabular information based on small populations or small cell counts (potentially identifiable information)*. Available at ukacr.org.uk/data-confidentiality-and-security : UKACR policies: identifiable data disclosure. Accessed 29.07.10.

five-year age groups between 0 and 24 years. In this age range, particular care should be given to tabulations, and aggregations should be made to avoid sparse cells.

In the case of eg geographical wards or aggregations of wards the total denominator population of an area may be smaller. In such cases, the release of tabular data based on this area should be governed by the principles listed in 5.2, and preparation and publication of any tables should follow the procedures outlined in 5.2–5.6. Release of geographical information that may, when combined with other data, yield information about non-contiguous areas with small populations should be treated in the same way as wards.

5.6 **Minimising risk with PII**

The following principles are based on the Office for National Statistics' guidance on minimising the risk of disclosure

- where the dissemination of certain data is covered by legislation, the provisions of that legislation must be met
- for the majority of health statistics, all cells with a marginal total of 1 or 2 should be considered unsafe. Care should also be taken where a row or column is dominated by zeros
- for more sensitive health statistics, all cells with a marginal total of 1 to 4 should be considered unsafe and care taken where a row or column is dominated by zeros. Higher levels of protection may be needed for small geographical areas or for variables with a particularly high level of interest and impact
- care should be taken when the same unit is represented more than once. (For example, if protection is required for practitioners then cells in a table where all the values relate to a specific practitioner could be disclosive.)
- disclosure risks may also increase if groups of statistical units (eg women attending a particular screening clinic) are represented in a table and could therefore identify each other
- the disclosure risk for event-based data will be different from residence-based data. (In order to identify an individual in a table for people visiting a screening clinic, for example, one would need to know that the individual attended the clinic.)
- the risk of disclosure can increase in linked tables if it is possible to differentiate or combine information using data available from other sources
- for some health statistics the likelihood of identification will be lower if tables are disseminated at a high level of aggregation and only limited tables are produced from the one database. (This will prevent users from linking current and future releases)
- disclosure is also less likely if the population base or the coverage of the table is not easily identifiable
- the age of the data may reduce the risk of disclosure because the population of the statistic will change over time.

A number of statistical techniques may be used to protect against disclosure. They fall into three categories: those that determine the design of the table, those that modify the values in a table, and those

that adjust the data before tables are designed. Where such techniques are deployed, users should be provided with an indication of the nature and extent of any modification this has involved. However, the level of detail should not permit the recovery of disclosive cell counts.

6. General issues

Written local policies and standard operating procedures should be in place to deal with the secure storage and transfer of patient- and staff-related confidential records within the NHS CSP. As a minimum standard, these policies and procedures must meet the requirements set out below.

6.1 Keeping patient information secure

Guidance on keeping patient information secure is set out in *Confidentiality: The NHS Code of Practice*, 2003 and summarised in Appendix 2 of this policy. Key points include the importance of not sharing passwords and of using individual log-ins, rather than shared or 'generic' ones.

6.2 Transferring records

Arrangements for transferring records will vary according to the sensitivity of the material they contain. As a minimum, the transmission of information should be restricted as follows

- by post
 - all external correspondence must be clearly and accurately marked with the name and address of the recipient
 - when posting sensitive material double envelopes must be used
 - sensitive or personal mail should be marked 'addressee only'
 - bulk person identifiable information (10 or more records) sent via mail must be sent using Royal Mail's 'Special Delivery' (or other secure courier service, according to local arrangements)
 - robust mechanisms are required for receipt and dispatch of all materials sent out for reporting (eg pathology samples or hard copy screening films being processed off site)
- by email/ electronic transfer
 - identifiable or potentially identifiable data transferred by electronic means must be sent separately from other information.
 - they should be encrypted or sent via nhs.net.
 - all passwords should be issued separately, preferably via telephone once the data are received
- by fax
 - the fax machine must be secure in a 'safe haven' area, with immediate collection and receipt confirmed
 - particular care should be taken to ensure that the fax number of the addressee is keyed in correctly
- by telephone
 - identifiable patient information must not be given to an unrecognised or unverified person over the telephone
 - where requests do not involve disclosure of IPI – eg a helpline caller seeking his or her screening due date – the identity of the caller should be verified in accordance with local procedures
 - where requests do involve the disclosure of IPI, the requester should always be called back to verify his/her

- identity and to check his or her right to access that information before releasing it
- all internal requests for identifiable patient information taken over the telephone must be recorded and logged
- external requests for identifiable patient information must not be accepted over the telephone but must be placed in writing
- databases
 - database demonstrations should make use of fictitious data.

7 Validity of this Policy

This policy is effective immediately and will be reviewed annually by the Programmes' Information Governance Committee before the NIGB/ECC application is renewed.

Glossary

DATA

Data

As defined in the Data Protection Act 1998 and related amendments, 'data' means information which

- is being processed by means of equipment operating automatically in response to instructions given for that purpose.
- is recorded with the intention that it should be processed by means of such equipment
- is recorded as part of a relevant filing system or with the intentions that it should form part of a relevant filing system
- forms part of an accessible record, or
- is held in unstructured or semi structured form by public authorities.

Anonymised data

This does not imply that data are 100% anonymous but that they are sufficiently anonymous (eg by the removal from records of the name, address and full postcode) to make the identification of an individual an extremely remote possibility.

Pseudonymised data

Data in which key identifiers have been systematically changed, enabling the individual to be identified from the original data list only by using a code or key.

Data controller

Person or people who determine how and for what purpose data are to be processed.

Data protection (principles enshrined in the Data Protection Act 1998)

Personal data shall be processed fairly and lawfully.

They 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.

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

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

They shall be accurate and, where appropriate, kept up to date.

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

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

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.

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

Individual to whom personal data relate.

Personal data

Data consisting of 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. It 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.

Sensitive personal data

Information on

- the racial or ethnic origin of the data subject
- his or her political opinions, including membership of a trade union
- religious (or other similar) beliefs
- physical or mental health or condition
- sexual life
- any offences actually or allegedly committed by the data subject, any proceedings arising from them, the decision and the sentence.

PATIENT INFORMATION

Confidential patient information

Patient information that was obtained or generated by a person who, in the circumstances, owed a duty of confidence to that individual.

Identifiable patient information (IPI)

Information from which the identity of the individual in question is ascertainable

- either from that information alone, or
- from that information and other information which is in the possession of, or is likely to come into the possession of, the person processing that information.

IPI includes

- the personal details of any patient or carer (eg name, date of birth, address, full postcode, telephone number, separately or in combination) or the hospital number or other unique identifiers of any health service patient, including the NHS number
- any information pertaining to the diagnosis, prognosis or treatment of an individual where this is linked to details that may enable that person to be identified

Potentially Identifiable Patient Information (PIPI)

'All items of information which relate to an attribute of an individual should be treated as potentially capable of identifying patients and hence should be appropriately protected to safeguard confidentiality' (Caldicott Committee, Report on the Review of Patient-identifiable Information, 1997).

Attributes such as occupation, gender, or ethnic group are PIPI, insofar as the identity of the individual in question may become ascertainable if these attributes are combined with other information which is in the possession of, or is likely to come into the possession of, the person processing that information.

The term PIPI is also used of individual level anonymised information or tabular information based on small populations or small cell counts, including: individual records; tabular data based on small geographic areas with cell counts of fewer than four or five cases or events (where the information is especially sensitive) or one to two cases (where it is not); tabular data containing cells that have underlying population denominators of less than approximately 1,000.

DISCLOSURE

This occurs when data held or information extracted from those data are passed (in any format) to someone other than the data controller.

FAILSAFE

A system designed to ensure that no-one eligible for screening is lost to the screening programmes.

PROCESSING OF DATA

Processing in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including

- organisation, adaptation or alteration of the information or data,
- retrieval, consultation or use of the information or data,
- disclosure of the information or data by transmission, dissemination or otherwise making available, or
- alignment, combination, blocking, erasure or destruction of the information or data.

Fair and lawful processing

Processing is fair and lawful when

- 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
- data sharing protocols comply with Data Protection Act 1998
- (in most cases) data subjects are informed about the identity of the data controller and uses of the data.

For further detail see

http://www.ico.gov.uk/for_organisations/data_protection_guide/key_definitions_of_the_dpa.aspx



Cancer Screening Programmes

APPENDIX 1 (COPY 1)

CONFIDENTIALITY AND DISCLOSURE POLICY DECLARATION OF COMPLIANCE

To be signed by an *authorised representative of:
any unit directly engaged in providing screening services to NHS Cancer Screening Programmes;
any organisation providing such services within one or more Trusts.
(*See section 1.3)

On behalf of

I declare that to the best of my knowledge, information and belief all employees of this unit/organisation who have or may have access to identifiable or potentially identifiable information relating to individual patients or NHS staff have read and undertake to comply with NHS Cancer Screening Programmes' Confidentiality and Disclosure Policy (2011).

Please **complete or delete** as applicable
Our access to these data is covered by an agreement dated
between
and

Signed
Name (print)
Role
Organisation
Date.....

Please **return** one signed copy to the programme lead and **retain** the second signed copy for your file.



Cancer Screening Programmes

APPENDIX 1 (COPY 2)

CONFIDENTIALITY AND DISCLOSURE POLICY DECLARATION OF COMPLIANCE

To be signed by an *authorised representative of:
any unit directly engaged in providing screening services to NHS Cancer Screening Programmes;
any organisation providing such services within one or more Trusts.
(*See section 1.3)

On behalf of

I declare that to the best of my knowledge, information and belief all employees of this unit/organisation who have or may have access to identifiable or potentially identifiable information relating to individual patients or NHS staff have read and undertake to comply with NHS Cancer Screening Programmes' Confidentiality and Disclosure Policy (2011).

Please **complete or delete** as applicable
Our access to these data is covered by an agreement dated
between
and

Signed
Name (print)
Role
Organisation
Date.....

Please **return** one signed copy to the programme lead and **retain** the second signed copy for your file.

APPENDIX 2 Keeping patient information secure

From *Confidentiality: The NHS Code of Practice*, 2003.

For all types of records, staff working in offices where records may be seen must

- shut/lock doors and cabinets as required
- wear building passes/ID if issued
- query the status of strangers
- know who to tell if anything suspicious or worrying is noted
- not tell unauthorised personnel how the security systems operate
- not breach security themselves.

Manual records must be

- formally booked out from their normal filing system
- tracked if transferred, with a note made or sent to the filing location of the transfer
- returned to the filing location as soon as possible after use
- stored securely within the clinic or office, arranged so that the record can be found easily if needed urgently
- stored closed when not in use so that contents are not seen accidentally
- inaccessible to members of the public and not left even for short periods where they might be looked at by unauthorised persons
- held in secure storage with clear labelling. Protective 'wrappers' indicating sensitivity – though not indicating the reason for sensitivity – and permitted access, and the availability of secure means of destruction, eg shredding, are essential.

With electronic records, staff must

- always log-out of any computer system or application when work on it is finished
- not leave a terminal unattended and logged-in
- not share logins with other people. If other staff have need to access records, then appropriate access should be organised for them – this must not be by using others' access identities
- not reveal passwords to others
- change passwords at regular intervals to prevent anyone else using them
- avoid using short passwords, or using names or words that are known to be associated with them (eg children's or pet's names or birthdays)
- always clear the screen of a previous patient's information before seeing another
- use a password-protected screen-saver to prevent casual viewing of patient information by others.