Public Health Agency

Data Protection / Confidentiality Policy Document

Main Author:
Consultation Route:
Approved By:
Date of Issue:
Applicable: Organisational wide
Version: 1.0
Review Date: February 2011

Version 1.0, February 2010

Amendment / Change Control

Date of Review	Changes Made	By Whom	Rationale/Driver	Authorised By

C O N T E N T S

1. INTRODUCTION

1.1 Data Protection policy - Background

The ease with which personal information can be passed within Health and Social Care (HSC), often by computer, is an undoubted benefit for patients and clients, for those involved in their care and treatment and in the planning and commissioning of Services. But all those concerned need to be aware that there is a legal duty to protect the confidentiality of personal information whether it relates to patients, clients, staff, members, etc.

The Public Health Agency (PHA) recognises that it has a responsibility to respect the individual's right for privacy and hence an expectation that information will be treated as confidential. This policy is based on that expectation and acknowledges that HSC staff will need to have strictly controlled access to personal information, anonymised wherever possible, to ensure that the HSC functions effectively and efficiently.

All PHA staff, agents and contractors are reminded of their responsibilities under Data Protection and Confidentiality. Breaches of confidentiality will be treated as a serious matter and may result in disciplinary action including dismissal, or in the case of an Agent or Contractor, consideration will be given to the termination of any formal arrangements.

1.2 Purpose of the Policy

This policy statement aims to clarify how and when personal information may be shared, the need to make patients, clients and staff aware of the ways in which their information might be used, and emphasises the use wherever possible of anonymised information setting out the circumstances in which information may be passed on for other purposes or as a legal requirement.

It also confirms and reinforces that a Common Law duty of confidence applies to everyone working for or with the HSC and aims to inform all staff working within the Public Health Agency of the personal role they must play in the protection and use of all personal information.

This policy should be read alongside the PHA's Facilities Management Policies for each location, which deal with the physical security of information held within the PHA and gives important guidance in this respect.

The policy has been written in line with current legislation and guidance on data protection, with particular reference to the Health and Social Services Executive's guidance document "Code of Practice on Protecting the Confidentiality of Service User Information" (January 2009) the Data Protection Act 1998 (Appendix VIII) and with reference to the Principles set out in the Caldicott Committee Recommendations (Appendix IX). "Professional staff employed by the PHA are reminded that their relevant

Professional Body will provide standards and guidance on confidentiality. Examples of such can be found on both the General Medical Council (GMC) and the Nursing and Midwifery Council (NMC) websites at the following links:
hhtp: //www.gmc-uk.org/guidance/index.asp
hhtp://www.nmc-uk.org.aSection.aspx?SectionID=11"
This policy is based on the following principles:

Governing Principles

a. That data access is confined to those with specified authority to view the data, i.e. **confidentiality**;

b. That all systems are operating correctly and that all information held is believed to be accurate and up-to-date, is collected and processed for specific purposes, is held only as long as is necessary for the purpose for which it was collected, is processed fairly and lawfully and is disposed of in a way which continues to protect confidentiality, i.e. **integrity**; and

c. That information is delivered to the right person when it is needed, i.e. **availability**.

The following governing principles are at the heart of this policy document, and should be viewed as the defining principles when handling personal data.

1 The Use and Transfer of Personal information within or from an organisation should be clearly defined, justified and regularly reviewed

2 Personal data items should not be included in transfers of information within or between organisations unless it is absolutely necessary and there is a robust business need

3 Only the minimum amount of identifiable information should be transferred or be accessible as is necessary for any given, specified and approved function

4 Only those individuals who need access to personal information should have access to it, limited to what they need to see for their particular business need.

5 Managers and 'Data Owners' should take such actions as are necessary on an ongoing basis to ensure that all staff are made fully aware of their contractual and legal responsibilities and obligations to respect and protect individuals personal information from unauthorised disclosure, loss or destruction.

6 Every use to which personal data is put, should be lawful and comply with all relevant applicable guidance

7 No personal information should be transferred within or between organisations unless adequate, robust and approved security mechanisms are in place

1.3 Definitions

The term “personal information” applies to “personal data/ information”, as is defined in law, about living individuals held in whatever form by or for Health and Social Care organisations, agents or staff. Personal data is data which relates to a living individual who can be identified from those data. This definition covers the obvious such as medical and staff records in addition to personal ‘non-health’ information such as a patient or client’s name and address or details of his or her financial or domestic circumstances. It relates to both computerised and manual records and can be held in different formats, and include, for example, CCTV images, microfiche audio recording or still photographic images

Data Controller
For the purpose of this document the Public Health Agency (PHA) is the “Data Controller”, and therefore, the organisation and its employees are subject to, and required to be compliant with, the principles set out in the 1998 Data Protection Act.
The Department of Constitutional Affairs defines the “Data Controller” as, “a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed”.

Personal Data Guardian

The role of Data Guardian is key to ensuring that the Public Health Agency satisfies the highest practical standards for handling personal information. The Guardian shall actively encourage work to facilitate, approve and enable legitimate information sharing, ensuring through the Information Governance function, that advise on options for lawful and ethical processing of information is available to the Public Health Agency and its officers. They will ensure the development of security and confidentiality policies.

The Personal Data Guardian will ensure representation of confidentiality requirements and issues at PHA board level.

Data Processor
The Department of Constitutional Affairs defines the “Data Processor”, in relation to personal data, as any person (other than an employee of the data controller) who processes the data on behalf of the “data controller”
In relation to the Public Health Agency, this definition would define, for example, The Business Services Organisation, as a PHA data processor.

Data Owner
See paragraph 3.2.8

In a legal context the Public Health Agency “owns” the “data” it “controls” and is responsible for ensuring compliance with the principles set out in the Data Protection Act 1998.

1.4 Further Information

Further information regarding this policy or any aspect of protection and use of personal information may be sought from the Information Governance Manager, the DHSSPS website or the Office of the Information Commissioner;

http://www.dhsspsni.gov.uk/
http://www.informationcommissioner.gov.uk/

2. BASIC PRINCIPLES

2.1 Every citizen has a right to privacy.

2.2 All PHA staff are legally bound by a Common Law duty of confidence to maintain confidentiality of information and abide by the principles of the Data Protection Act 1998.

2.3 Information provided in confidence may not be used for a purpose other than that for which it was collected or be passed to anyone else without the consent of the provider of the information. If occasion arises where it is proposed that personal information be used for another purposes, then expert opinion should be sought before any processing takes place.

2.4 Patients, Clients and staff should, where it is reasonable and practicable to do so, be informed in advance of the uses to which their information may be put. (Fair Processing Notices)

2.5 Patients and Clients' right to refuse the use of their information must be respected (except in exempted circumstances where this is required by law).

2.6 The PHA is legally morally and ethically bound to comply with all legislation and guidance relating to the protection and use of information

2.7 Access to, and release of, personal information will be strictly controlled; where possible anonymised and aggregate information will be used. Only the minimum data required will be processed by the PHA

2.8 Personal information will be held only for as long as it is required for the purpose for which it was collected. It will be disposed of in a manner that continues to protect confidentiality. Patients, Clients and Staff should be informed at the outset, the period that their information will be retained for,

2.9 Contractors with access to personal information held by, or on behalf of, the PHA, are required to comply with this policy, and have in place their own complimentary policies and procedures that will provide the same or greater protection to information processed on behalf of the PHA. The PHA will require that Contractors or Agents acting at the direction of the PHA, provide assurances and evidence this requirement.

3. PROTECTION AND USE OF INFORMATION

3.1 Uses and restrictions

3.1.1 Patients, clients and staff should be advised in advance of the uses to which the information they provide may be put. This may be verbally, in written form on standard documentation used to collect information or on literature on protection and use of

personal information designed specifically for this purpose. These are known as Fair Processing Notices.

3.1.2 Personal information may in appropriate circumstances * be used for:

- The delivery of personal care and treatment, including needs assessment and Service Planning
- For assuring and improving the quality of care and treatment.
- To monitor and protect public health including the prevention and control of disease.
- To co-ordinate HSC care with that of other associated agencies.
- For effective Health and Social Care administration.
- Teaching, Training and Education of Staff.
- In statistical analysis and Medical or Health and Social Care research.
- Staff Administration and records including pay, superannuation, work management and discipline
- Accounting and Auditing including the provision of accounting and related services, the provision of an Audit where such an audit is required by statute.
- Crime prevention and prosecution of offenders
- The administration of licensing or maintenance of official registers
- Benefits, grants and loans administration
- Investigation of Complaints
- Defending Legal Challenge
- Auditing of Bodies in receipt of monies from the Public Health Agency
- Auditing of processes carried out at the direction of the Public Heath Agency by external Agents or Contractors

*** Note**: If unsure whether or not a particular use is covered by the above, advice should be sought from the Information Governance Manager.

3.1.3 Sometimes personal information is required by statute or court order and the PHA will be obliged to release the information in these circumstances.

3.1.4 Release of information in relation to protection of the public, tackling serious crime are covered by the “”Code of Practice on Protecting the Confidentiality of Service User Information” (January 2009) which should be studied in conjunction with this policy.

3.1.5 The PHA will not permit personal details to be released or sold on for fundraising or commercial marketing purposes. The PHA does not, nor does it permit external Agents or Contractors to pass on information to third parties unless the purpose is legitimate and express written consent has been given by the PHA.

3.2 Collection, Retention and Disposal of Information

3.2.1 Data subjects will be advised of the uses to which their information may be put. This should take the form of information to patients & clients as laid out in the DHSS ”Code of Practice on Protecting the Confidentiality of Service User Information” (January 2009)They will also be advised on request of the rights of access which apply to certain records under the Data Protection Act 1998.

3.2.2 Information sharing between HSC bodies may require a signed Data Access Agreement between the parties. It is recommended that such an agreement is in place for those information flows regularly shared, for example, between the PHA and their Providers. A sample Data Access Agreement is included (Appendix I.)

3.2.3 Information sharing between HSC bodies and non-HSC bodies must also be covered by a Data Access Agreement.

3.2.4 Patients or Clients who consider withholding or restricting transfer of information should be advised that such restriction could possibly have an adverse impact on their care or treatment as the sharing of personal information, is often critical to ensure that the highest level of service is afforded to the individual. Legal or statutory requirements should also be explained. HSC staff should ensure that these discussions are handled with sensitivity and care and that the opinion of the individual is respected when making decisions about the use to which their information is to be put.

3.2.5 Only sufficient information for the purpose/s will be collected.

3.2.6 Computerised personal information will be held on systems that are at the very least password protected and comply with the PHA ICT security policies and to which access is restricted to authorised personnel. Guidance on use of passwords is laid out in the PHA ICT Security Policy

3.2.7 Removable media such as fob keys and laptops should have encryption software installed to protect against unauthorised access to sensitive information in the event of a loss or theft of that equipment. It is not permitted to store or transfer sensitive information, either corporate or personal, on media that is not encrypted.

For security purposes each electronic or physical set of data should be assigned an "owner". The data owner will be responsible for:-

- Identifying all the data within the area of responsibility;
- Specifying how the data can be used;
- Agreeing who can access the data, and what type of access each user is allowed. See Appendix I for PHA 'Data Access Agreement Form'.
- Determining the classification or sensitivity level(s) of the data;
- Periodically reviewing that classification;
- Ensuring and Approving appropriate security protection for the data, eg. encryption software
- Ensuring compliance with security controls;
- Ensuring compliance, where necessary, with the Data Protection Act (1998), and any other relevant legislation covering personal or medical data.

Data classed as sensitive within one system should maintain at least the same sensitivity level across all systems.

Access rights given to users should be consistent across all areas. Particular attention should be paid to data being downloaded to a computer. Corporately sensitive information often ceases to be sensitive after a period of time, for example, when the information has been made public. This should be taken into account, as over-classification can lead to unnecessary expense.

Please note: It is advised where possible that personal or business sensitive information should not be held on desktop or laptop computers. Such information should be held on a server to mitigate risk in the event of a loss or theft of that equipment.

3.2.8 Manual personal information will be held securely, for example in locked filing cabinets, and access restricted to authorised staff. Access will be granted at the direction of the data 'owner' (see 3.2.6)

3.2.9 Staff should operate a clear desk policy whereby personal information is not left in clear view of others.

3.2.10 Information will be retained only for as long as the purpose/s requires it bearing in mind legal timescales for retention of particular records (Appendix II). Individual departments within the PHA are required to be familiar and comply with the timescales under which the personal information they hold is governed. Reference should be made to the DHSSPSNI document "Good Management Good Records" and the PHA "Records Management Policy" document and the PHA "Retention and Disposal Schedule".

3.2.11 Methods used for disposal of confidential information must continue to protect confidentiality. Paper information should be shredded by means of a 'chip' or 'confetti' shredder. It is not permitted to shred sensitive information by means of a 'strip' shredder as this method is no longer considered secure.
Prior to being discarded, all removable storage media that may contain sensitive or valuable information should be degaussed or by other means rendered unusable. Media to be degaussed or otherwise destroyed should be held securely until collected. . Advice should be sought from the BSO I.T. Officers regarding all matters of media destruction. Officers responsible for the formal disposal of media, should ensure that a disposal certificate is sought from any contractor employed to carry out this task. Further information on this area can be found in the PHA Waste Management Policy.

3.3 Processing and Presentation

3.3.1 Staff who are authorised to do so will process and present information in line with uses and restrictions set out in 3.1

3.3.2 Information will be presented in an aggregate, anonymised form where disclosure of individuals information would not be authorised for the purpose. Anonymisation does not in itself remove the duty of confidence in relation to the information. Confidentiality must still be protected.

3.3.3 With increasing usage of geographical information mapping tools (GIS) it is important to emphasise that, within the PHA, mapping systems are utilised only by trained staff who are fully aware of their personal responsibilities in protecting individual information from disclosure, both in its raw form and in any way in which it is potentially represented.

3.3.4 Information labelling and handling.
Sensitive information should be labelled appropriately and output from systems handling such data should carry an appropriate classification label (in the output). The marking should reflect the classification of the most sensitive data in the output. Output includes all types of storage media and file transfers.

The document ”Code of Practice on Protecting the Confidentiality of Service User Information” issued by the DHSSPSNI in January 2009 deals with the handling of personal information. Care should be taken to meet its requirements. The document can be found at the following web address: www.dhsspsni.gov.uk/confidentiality-code-of-practice0109.pdf

3.4 Disclosure

3.4.1 Disclosure of personal information will be on a strictly “need to know” basis and in accordance with the uses detailed in 3.1 and where necessary, in consultation with the data ‘owner’ (see 3.2.6)

3.4.2 Information disclosed will be minimalist, i.e. only that essential to the purpose of the authorised user will be released from a core data set

3.4.3 All requests for information should be logged and disclosure of personal information authorised by a nominated individual within the department. This may be the ‘owner’ or local records manager Where doubt arises on disclosure of particular information, advice should be sought from the Information Governance Manager or designated Data Guardian.

3.4.4 Where information has been sought for research purposes by external organisations/individuals, a Data Access application should be issued and returned before an informed decision is taken on appropriateness of disclosure. (appendix III)

3.4.5 For some guidance in relation to the risks associated with information requests, refer to the Department’s revised ”Code of Practice on Protecting the Confidentiality of Service User Information” (January 2009)

3.4.6 In line with guidance laid down in the PHA’s ICT Security Policy and various protocols operating within the Agency, disclosure of any information must be via media appropriate to the sensitivity of the information concerned. Security measures such as passwords and encryption must be employed when transferring or storing personal or corporately sensitive data and must be authorised by the department’s nominated individual or the data ‘owner’. Further advice can be sought from the Information Governance Manger or your IT Officer.

3.5 Data Access Requests

Data subjects have the right to see or request a copy of data which is held about them, whether this be computerised or manual. The current maximum charge applicable for access is £10 for records held on computer and £50 for paper records or other media (e.g. X-ray). All requests must be received in writing. The procedures for dealing with such requests are laid

out at Appendix IV. Further advice may be sought through the Information Governance Manager.

3.6 Information for Statistics and Research

Policies and procedures exist for the sharing of information in controlled circumstances for statistics and research purposes. The Body / Organisation requesting information is required to complete an 'Application for Access to Personal Level Data for Research Purposes' which must be submitted to the PHA. The PHA would follow the lines of approval prior to any information being released. A data access agreement would be drafted to cover any disclosure. Note; Using information for research purposes is addressed within the Data Protection Act 1998, however, strict guidelines will apply, and appropriate safeguards must be present, in order for data to be used for research purposes. Further advice may be sought from the Information Governance Manager or designated Data Guardian.

3.7 Human Resources Records

Personal information is collected for recruitment purposes, for salaries and wages, for maintenance of the employment relationship between the PHA and its staff and to ensure that the PHA complies with its HR policies and procedures. HR policies are available on the PHA Intranet site. It is important to recognise that any staff information held by managers should be afforded the highest levels of privacy and security. It should be noted, that rights afforded to the individual under the Data Protection Act 1998, extend to employees of the PHA and these rights are not lessened by virtue of the employer / employee relationship.

3.8 Audit Records

The PHA is required to provide access to all its records to
Internal Audit. This access pertains to all records, documents and correspondence relating to any financial or other relevant transaction, including documents of a confidential nature. This disclosure of information is covered by the PHA's Data Protection registration with the Information Commissioner and Internal Auditors are contractually bound to maintain the security and confidentiality of all records in their keep as with all personal information held by the PHA. Further to this, The Comptroller & Auditor General under powers conferred to his Office through the introduction of the 'Audit and Accountability (Northern Ireland) Order 2003' will periodically require disclosure of information from the HSC. It should be noted that the HSC is legally bound to comply with any request for access to information held on both employees and contractors. Release of such information does not require the consent of the individuals concerned under the Data Protection Act 1998. For further information on this matter, please contact the Information Governance Manager:

3.9 Responsibilities of Staff and Contractors

3.9.1 All staff are bound contractually to protect the confidentiality of information to which they have access in the course of their employment, see contract extract Appendix V

3.9.2 Provision currently exists in contracts between the PHA and Providers to maintain confidentiality of information that is utilised in any dealings arising from the operation of the contract (Appendix VI). Providers should ensure that any information disclosed to the PHA is anonymised where possible. Where identification of individuals is necessary, Providers should ensure that appropriate consent of data subjects is in place for the purpose of disclosure and that disclosure is in line with the provisions of all relevant legislation and applicable guidance

3.9.3 Comprehensive confidentiality clauses are currently written into contracts between the PHA and Computer Companies/Agencies and general maintenance contractors which refer directly to the protection of personal data and confidentiality; **Appendix VII(a/b).**
All contractors have a responsibility under this policy and existing legislation to protect the information to which they have access under the terms of their contract.

3.9.4 Protocols, such as those for faxing information and operation of 'safe haven' addresses and associated contact persons, are currently shared with those Providers/contractors to whom they may apply.

3.10 Out of the Office

It is PHA policy that patient/client-identifiable information is stored on-site where possible. The PHA expects that no patient, client or employee identifiable information will be removed from the building without the approval of a sufficiently authorised officer. Note Security measures such as passwords and encryption software should be present before any decision to allow information to leave the premises is taken. Reference should be made to the PHA's ICT Security Policy.

3.11 Breaches of policy

3.11.1 All staff, contractors and agents are reminded that they are bound by a Common Law duty of confidence in the protection and use of personal patient, client and staff information. All staff contractors and agents should be aware of and abide by the contents of this policy.

3.11.2 **Any suspected breach of this Policy must be reported to the Information Governance Manager immediately, or by contacting another member of the Information**

Governance Team. The incident can then be assessed and appropriate corrective action can be taken.

4. PHA BOARD RESPONSIBILITIES

4.1 Management Arrangements

4.1.1 The PHA board has approved this policy document in recognition of its responsibilities in relation to the protection and use of personal information.

4.1.2 The PHA board requires that Management make appropriate arrangements to ensure communication of this policy to all levels of staff within the organisation, and ensure that staff attend training courses relating to this particular subject.

4.1.3 Any queries arising in relation to this policy should be directed to the Information Governance Manager

4.2 Resources

4.2.1 The PHA board will consider the use of resources in developing materials to inform patients, clients and staff of the uses to which their information will be put and to their rights of access where appropriate.

4.2.2 Training to communicate the responsibilities laid out in this and associated policy documents and practical measures that can be taken to comply with the contents will be provided for all PHA staff

4.2.3 Practical guidance for compliance with this policy and the ICT Security Policy will be provided for all staff. This information will also be provided on hardcopy and through the PHA Intranet site.

4.2.4 It is envisaged that all new staff will be informed of their responsibilities in relation to this policy and the ICT Security Policy as part of the PHA induction to the organisation. All new staff will sign to indicate receipt of both Policies. All Managers will be responsible for ensuring staff are familiar with both policies and are aware of their responsibilities in relation to their particular business activity.

4.2.5 Periodically, internal audit will review the PHA's arrangements for adequately protecting and appropriate usage of personal information.

4.2.6 Information Governance Manager will make arrangements for periodic 'audits' of the buildings to ensure that all staff are familiar with and abiding by the contents of the policy and its

associated guidance. Reports on these audits will be prepared for consideration by the relevant committees of the PHA

4.2.7 Contractors will be made aware of the contents of this policy and their associated responsibilities. In addition, they will be required to provide the PHA with their own policy guidelines relating to the protection and use of patient, client and staff information, and provide assurances that they will abide by their legal responsibilities.

4.3 Ensuring Adherence

4.3.1 Through effective communication, the PHA requires that staff act responsibly and within the confines of this policy document. However, breaches will be dealt with as serious matters and the PHA will not hesitate in exercising its rights in such situations.

4.3.2 Contractors working with or on behalf of the PHA will be informed that they too are bound by the principles laid down in this policy and the relevant clauses included in all contracts.

4.4 Review of policy

4.4.1 This policy will be periodically reviewed and updated to ensure that it is in line with current guidance and legislation relating to protection and use of patient and client information. This policy will be reviewed no later than February 2011.

APPENDICES

HSC Public Health Agency

REF. NO:

Appendix I
PHA
DATA ACCESS AGREEMENT

THIS AGREEMENT AUTHORISES THE IMPLEMENTATION OF ACCESS TO THE DATA SPECIFIED BELOW (PART A) BY THE ORGANISATION INDICATED IN PART B.

PART A:

DATE ACCESS BEGINS _____ **DATE ACCESS ENDS** _____

REVIEW DATE _____

(A review date MUST be entered)

What machine/application holds the data to be accessed?

Machine _____ Application _____

What data is to be accessed?

_____

Is the data to be Viewed only (V); or viewed and updated (U); or Transferred and viewed(T)? _____

How is the data to be accessed?
_____

Please state purpose for which data will be used?
_____

What measures are in place to ensure the security of the data once received? _____

PART B: ON BEHALF OF THE ORGANISATION WISHING TO ACCESS THE DATA

I CONFIRM THAT:-

My organisation requires access to the data specified in Part A above, and will conform to the Data Protection Act, 1998 and the guidance set out in the DHSSPSNI"Code of Practice on Protecting the Confidentiality of Service User Information" (January 2009)

- Signed for and on behalf of (HSC only)

Signature _____

Name (Block Caps) _____ Date _____

- **The signatory must carry the specific authority of the Chief Executive/ or equivalent.**

PART C: (TO BE COMPLETED BY THE DATA CONTROLLER)

I CONFIRM THAT:-

1. My organisation consents to the disclosure of the data specified in Part A to the organisation specified in Part B;

2. The data covered by this agreement are:-
   - Either data which are exempt from the Data Protection Act, 1998, or
   - Are notified under the Data Protection Act, 1998 and their disclosure

     conforms to the current notification under the Act;

3. The disclosure of the data conforms to the "Code of Practice on Protecting the Confidentiality of Service User Information" (January 2009)

- Signed for and on behalf of (HSC only)

Signature _____

Name (Block Caps) _____ Date _____

- **The signatory must carry the specific authority of the Chief Executive/Data Guardian or equivalent. Or have specific delegated authority from one of those officers listed**

PART D. FOR DIS USE ONLY – NOTES (*where applicable)*

PART E. FOR DIS USE ONLY *(where applicable)*

ACCESS AUTHORISATION
(Deputy Director, or in his absence, PO)

Signature _____

Name (Block Caps) _____ Date _____

Appendix II
RETENTION OF RECORDS

The retention and disposal of Agency records must be in line with both the Agency's Records Management Policy and the corresponding Retention and Disposal Schedule. The Retention and Disposal Schedule is based on the DHSSPS publication 'Good Management, Good Records' and outlines minimum retention periods for records created in the Agency. The Schedule also details the final action for Agency records by identifying those which need to be transferred to the Public Record Office for Northern Ireland (PRONI) and those which can be destroyed once they have been retained for the sufficient period of time.

Appendix III

APPLICATION FOR ACCESS TO PERSONAL LEVEL DATA FOR RESEARCH PURPOSES

1. Personal Details – Researcher / Planner

Surname :_____

Forenames :_____

Postal Address :_____

_____

_____

Postcode:_____

Organisation :_____

Telephone No. :_____

Fax No. :_____

Email :_____

2. Project Details

Title of Project :_____

_____

Project purpose:_____

/ background _____

_____

_____

_____

_____

_____

_____

Proposed Start Date : _____

Duration : _____

3. Approval sought by the Researcher / Planner

Identify organisations or individuals from which assurances of co-operation will be required and whether these assurances have yet been given

Name of individual/organisation and contact name	**Co-operation confirmed (Y/N)**

Has this research been cleared by the Ethical Committee (where appropriate): _____

(*copy of authorisation to be attached to this application)*

Terms and Conditions of Support

The following are the Terms and Conditions under which the Public Health Agency (PHA) will consider supporting the proposed research:

4. GENERAL CONDITIONS

4.1 The Applicant will acknowledge the support of the PHA in any final report

4.2 The Applicant will provide the PHA with an opportunity to contribute to the design of the research

4.3 The Applicant will provide the PHA with a presentation of the findings of the research if requested to do so

4.4 The Applicant will comply with all Data Protection requirements and will exercise proper safeguards to prevent any breach of confidentiality and/or privacy. Any disclosed results of the research shall not be able to identify an individual without that individual's written consent.

4.5 Data made available by the PHA to the Applicant is done so in confidence solely for the purpose of the above research project.

4.6 Data made available by PHA to the Applicant directly will not be divulged to any individual not associated with the research

4.7 When the research project is concluded, all personal data will be entirely destroyed.

4.8 The Applicant will provide the PHA with a pre-publication draft of any report generated from the research prior to publication.

4.9 The Applicant will pay for any reasonable costs incurred by the PHA in supporting the research, including costs incurred by other organisations.

5. AGREEMENT (To be completed by the Researcher / Planner)

I agree to the terms and conditions laid out in this document.

Signed

Project Leader: _____

Organisation: _____

Date: _____

6. Declaration of Data Protection Co-ordinator and Data Custodian

I declare that the Public Health Agencys involvement in the above research complies with the Data Protection Act and that all notification requirements have been completed.

Signed: _____ (Data Guardian)
Date: _____

Signed: _____(Information Governance Manager)
Date: _____

6.1 Chief Executive PHA (or Designated Deputy)

Signed: _____ (Chief Executive/Deputy)
Date: _____

Appendix IV

Procedure for dealing with subject access requests

Sample Letter

Information Governance Department
ADDRESS

Dear Sir / Madam

The Data Protection Act 1998 (DPA), gives everyone the right to seek access to their own personal information.

To request access to Health and Social Care records held by the Public Health Agency, please complete the attached 'application form' (2 pages). A letter of application is also acceptable (e.g. from a Solicitors office) but it should provide us with all necessary information to allow us to search for any relevant records.

Please include as much detail as possible about the records you are seeking e.g. type, location or any reference number you may have received from the Public Health Agency during previous correspondence.

The completed Application Form or letter of application should be returned along with;

a) A valid form of identification (e.g. driving licence, birth certificate, ID card, passport. – originals will be returned)
b) If the application is from someone other than the subject of the information, signed consent from the data subject
c) The relevant fee (see Application Form)

I am required to inform you that the 40 days, allowed under DPA, to process your request will not commence until we receive the applicable fee and all necessary documentation as indicated above.

If you have any queries about completing this Application Form, or about our procedures for processing such requests, please do not hesitate to contact me at the address provided.

Yours Sincerely

_____

Public Health Agency

Application for access to personal Health and Social Care records

(the relevant fee [see below] and a valid form of identification should accompany all request; see form for details of any documentation required to validate your application)

PART A

Your details (person to whom the information relates)

Surname Forenames

Date of Birth Other identifying Information

Address

Tel / Contact Number

If the details provided above are different from those that we may hold about you, please provide us with the following information

Previous Surname (1)_____ (2) _____

Previous Address (1)_____ (2) _____

Applicable dates _____

To help us identify the records you are seeking, please indicate what type of record you believe we may hold (eg Complaints records , Health records)

PART B I require access to the records in the following format: Fee required Please Tick

I only wish to view my records	FREE
Printout of records held on computer systems	£10

A copy of Social Services Records (paper records only) £10

A copy of Health care Records (paper records) and/or copies

Of X-Ray film £30

Note: A maximum of £50 is applicable for any combination of the above. All cheques should be made payable to the Public Health Agency

Part C Applicant's details (if not the person to whom the data relates)

If you are applying to see records that are not your own, please provide details:

What is your relationship to the person to which the information relates

Your surname Your Forenames

Your Address

Your Tel / Contact Number

(this is the address to which a reply or other correspondence will be sent, unless otherwise stated)

Please indicate below,by ticking relevant box,or deleting as appropriate

I have been asked to act on behalf of the person whose information is being sought and their written permission is included (Part E below) ☐

I am acting in parental capacity as the person whose information is being sought is under 16 years of age and: is incapable of understanding the request* OR has consented to my making this request*
(*delete as appropriate)

The person is over the age of 16, however is incapable of understanding the request and I therefore act as his/her personal representative ☐

The person is deceased and I am the next of kin ☐

The person is deceased and I am his/her personal representative and attach legal documents confirming my position ☐

PART D To be completed by the person requesting access to records

I declare that the information given by me is correct to the best of my knowledge and that I am entitled to request access to the records detailed above.

_____ _____
_____/_____/_____
Print Name(capitals) Signed Date

PART E To be completed by the person to whom the information relates to authorise release of records to the individual named at **PARTC**

I hereby authorise the Public Health Agency to release the records detailed on this form to

_____(representative named at **PART C**)

Signed_____
Date_____
(person to whom information relates)

Appendix V

CONFIDENTIALITY AS DETAILED IN STAFF CONTRACTS

CONFIDENTIALITY

You shall not as an employee of the PHA, or following the termination of your employment with the PHA, disclose other than to authorised person or in the course of duty without lawful authority, any matter or information which you have obtained or to which you have had access, owing to your official position. Breaches of confidence may result in disciplinary action, which may involve dismissal, or possibly render you liable to Criminal Proceedings

CONFIDENTIALITY OF INFORMATION HELD ON COMPUTERS

Your personal data will be held by the PHA on manual and computer records and will be processed in accordance with the Data Protection Act 1998. Further information is available from the Personnel Department. You are also advised that you have a statutory obligation under principle 7 of the Data Protection Act to protect any personal data to which you have access in the course of your employment. Any employee who unlawfully discloses personal data may be subject to disciplinary action by the PHA. You should also be aware that regardless of any action by the PHA, unauthorised disclosure of personal data could render you liable to Criminal Proceedings/Civil Action under the Data Protection Act 1998.

Appendix VI

Confidentiality in Provider contracts

The Protection and Use of Patient and Client Information

Any organisation who under formal agreement provides services for the PHA will be expected to follow DHSS&PS ”Code of Practice on Protecting the Confidentiality of Service User Information” (January 2009)and the recommendations and principles set out in the Caldicott Committee Report. Arrangements should be continually reviewed to ensure ongoing compliance with above named guidance and any further guidance issued. In addition all providers will be required to comply with the Data Protection Act 1998 and all other relevant and applicable legislation.

Public Access to Information about the HSC

The provider will be required to comply with the provisions of the Freedom of Information Act 2000 and provide whatever assistance is required by the Public Health Agency to allow it to meet its statutory obligations under this Act

Appendix VII (a)

CONTRACTORS AND CONFIDENTIALITY

CONTRACTS WITH COMPUTER COMPANIES

14. Confidentiality

14.1 Without prejudice to the application of the Official Secrets Acts 1911 to 1989 to any Confidential Information the CONTRACTOR acknowledges that any Confidential Information obtained from or relating to the Crown, its servants or agents is the property of the Crown.

14.2 The CONTRACTOR acknowledges that it has access to and will regard as Confidential Information all data of whatever nature relating to patients.

14.3 In further consideration of the AUTHORITY executing this Agreement with the CONTRACTOR, the CONTRACTOR hereby warrants that:

14.3.1 the CONTRACTOR (and any person employed or engaged by the CONTRACTOR in connection with this Agreement in the course of such employment or engagement) shall only use Confidential Information for the purposes of this Agreement;

14.3.2 the CONTRACTOR (and any person employed or engaged by the CONTRACTOR in connection with this Agreement in the course of such employment or engagement) shall not disclose any Confidential Information to any third party without the prior written consent of the AUTHORITY;

14.3.3 the CONTRACTOR (and any person employed or engaged by the CONTRACTOR in connection with this Agreement) shall take care at all times of all media, including storage media (including the data thereon) and all papers (including patient records), placed in its possession for the purpose of this Agreement. The CONTRACTOR hereby acknowledges that it has access to and will regard as Confidential Information all data of whatever nature relating to patients and Clients and undertakes to keep the AUTHORITY indemnified against all proceedings, actions, claims, demands, expenses and liabilities whatsoever arising out of breach of this Clause by itself, its servants, agents and sub-contractors and the servants and agents of

such sub-contractors. The CONTRACTOR also hereby acknowledges that the Computer Misuse Act 1990 is particularly relevant with regard to this Agreement.

14.3.4 the CONTRACTOR shall take all necessary precautions to ensure that all Confidential Information is treated as confidential and not disclosed (save as aforesaid) or used other than for the purposes of this Agreement by the CONTRACTOR's employees, servants, agents or sub-contractors; and

14.3.5 without prejudice to the generality of the foregoing neither the CONTRACTOR nor any person engaged by the CONTRACTOR whether as a servant or a consultant or otherwise shall use the Confidential Information for the solicitation of business from the AUTHORITY or another part of the Crown by the CONTRACTOR or by such servant or consultant or by any third party.

14.4 The AUTHORITY:

14.4.1 shall treat as confidential all Confidential Information obtained from the CONTRACTOR (see sec; 35.1.1 and 35.1.2)

14.4.2 shall not subject to Clauses 14.6 and 35, disclose to any third party without firstly giving consideration to consulting with the CONTRACTOR any Confidential Information obtained from the CONTRACTOR. (see sec; 35.1.1 and 35.1.2)

14.5 The provisions of Clauses 14.1, 14.3 and 14.4 shall not apply to any information which:

14.5.1 is or becomes public knowledge other than by breach of this Clause 14;

14.5.2 is in the possession of the receiving party without restriction in relation to disclosure before the date of receipt from the disclosing party;

14.5.3 is received from a third party who lawfully acquired it and who is under no obligation restricting its disclosure.

14.5.4 is independently developed without access to the Confidential Information.

14.6 Nothing in this Clause shall be deemed or construed to prevent the AUTHORITY from disclosing any Confidential Information obtained from the CONTRACTOR:

14.6.1 to any other department, office or agency of the Crown, provided that the AUTHORITY has required that such information is treated as confidential by such departments, offices and agencies, and their servants or agents, including requiring servants or agents to enter into a confidentiality undertaking where appropriate; and

14.6.2 to any consultant, contractor or other person engaged by the AUTHORITY in connection herewith, provided that the AUTHORITY shall have obtained from the consultant, contractor or other person a signed confidentiality undertaking on substantially the same terms as are contained in this Clause.

14.7 Nothing in this Clause 14 shall prevent the CONTRACTOR or the AUTHORITY from using data processing techniques, ideas and know-how gained during the performance of this Agreement in the furtherance of its normal business, to the extent that this does not relate to a disclosure of the AUTHORITY's Data, any data generated from the AUTHORITY's Data, a disclosure of any Confidential Information, or an infringement by the AUTHORITY or the CONTRACTOR of any Intellectual Property Right.

Protection of Personal Data

33.1 The CONTRACTOR's attention is hereby drawn to the Data Protection Act 1984 and the Data Protection Act 1998 (together the "Data Protection Acts").

33.2 Both parties warrant that they will duly observe all their obligations under the Data Protection Acts which arise in connection with this Agreement.

33.3 Without prejudice to the generality of Clause 33.2 and with reference to Schedule 1 Part II Paragraph 12 of the Data Protection Act 1998, the CONTRACTOR, as data processor, shall:

33.3.1 act only on instructions from the AUTHORITY, as data controller, and

33.3.2 take appropriate technical and organization measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Publicity

34.1 Except with the written consent of the AUTHORITY, the CONTRACTOR shall not make any press announcements or publicise this Agreement in any way.

34.2 The CONTRACTOR shall be permitted to name the AUTHORITY as a customer in responses to requests for information or responses to invitation to tender provided by Government Departments, Agencies or other Government bodies or organisations. Names and contact details of AUTHORITY personnel shall not be supplied without the AUTHORITY's prior written consent.

34.3 The AUTHORITY shall provide the CONTRACTOR with a copy of any media announcement, prior to its release, in respect of the CONTRACTOR's role or performance in respect of this Agreement.

35. Disclosure of Information

35.1 Notwithstanding the provisions of Clause 34, the AUTHORITY shall be entitled to disclose any information relating to this Agreement without consulting the CONTRACTOR in the following circumstances:

35.1.1 for the purpose of any examination of this Agreement by the National Audit Office pursuant to the National Audit Act 1983 or otherwise;

35.1.2 for parliamentary, governmental, statutory or judicial purposes; or in relation to any other legal or quasi legal obligation on the AUTHORITY, such as FOI or EIR legislation, or where/when a "public interest test" may apply

"Confidential Information" means all information designated as such by either party in writing together with all other information which relates to the business, affairs, products, developments, trade secrets, know-how, personnel, customers and suppliers of either party or information which may reasonably be regarded as the confidential information of the disclosing party.

Appendix VII (b)

CONTRACTORS AND CONFIDENTIALITY

General Maintenance

The Contractor, his employees and Agents shall at all times keep confidential and secret and shall not disclose to any person other than a person authorised by Business Services Organisation or the Public Health Agency all information and other matters acquired by the Contractor, his employees and Agents during the course of the works.

Statutory Obligations

The Contractor shall comply with all current statutory obligations and any amendments to those obligations as they may arise during the term of this contract. The Contractor shall comply with, and give all notices required by, any statute, any statutory instrument, rule or order or any regulation or by-law applicable to the work and shall pay all fees and charges in respect of the work legally recoverable.

Official Secrets and Confidentiality

The contractor shall take all reasonable steps to ensure that all persons employed by him or his subcontractors in connection with the Contract are aware of the Official Secrets Act 1989 and, where appropriate, of the provisions of Section 11 of the Atomic Energy Act 1946, and that these Acts apply to them during the execution of the Works and after the completion of the Works or earlier determination of the Contract.

Any information concerning the Contract obtained either by the Contractor or by any person employed by him in connection with the Contract is confidential and shall not be used or disclosed by the Contractor or by any such person except for the purposes of the Contract.

Appendix VIII

DATA PROTECTION PRINCIPLES, 1998 ACT

The principles of protection of personal data are contained within the Data Protection Act 1998. These impose specific requirements on PHA staff when handling Personal Data.

First Principle: 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 is met.
- In the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

(NB: HSC data are by nature sensitive data and consequently require grounds drawn from both schedules to justify processing. In legal terms, if data subject consent, explicit or otherwise, is lacking, then performance of functions under enactment of government functions or performance of a medical function may suffice.)

Second Principle: 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.

Third Principle: Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Fourth Principle: Personal data shall be accurate and, where necessary, kept up to date.

Fifth Principle: Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

Sixth Principle: Personal data shall be processed in accordance with the rights of the data subjects under this Act.

Seventh Principle: 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.

Eighth Principle: Personal data shall not be transferred to a country or territory outside the European Economic Area, 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.

More detailed information on the Data Protection Act 1998 is available from the Information Governance Manager or the Information Commissioners website at www.ico.gov.uk

Appendix IX
The Caldicott Principles (Best Practice)

The principles for dealing with patient-identifiable information are:

1) Justify the purpose.
   All uses of patient identifiable information should be clearly defined. The Caldicott Guardian should keep these uses under review.

2) Don't use patient identifiable information unless it is absolutely necessary.
   This includes within practices and primary care groups as well as where information is transferred between NHS organisations.

3) Use the minimum necessary patient identifiable information
   Where it is necessary to identify the patient you should use the minimum information required. For example could just an NHS number be used or surname and date of birth?

4) Access to patient identifiable information should be on a strict need to know basis
   Access to patient data should be restricted to those who need to know it, and then they should only have access to the data they need. Security measures should be introduced in practices and all NHS organisations to restrict access to patient data.

5) Everyone should be aware of their responsibilities
   Everyone who handles any patient information (from which individuals can be identified) should be appropriately trained in respect of patient confidentiality.

6) Understand and comply with the law
   Each organisation should have an individual who is responsible for ensuring that legal requirements are met. This includes the Data Protection Act and other relevant legislation.