OFFICE USE ONLY

Sys No
STH
System Owner

Sheffield Teaching Hospitals NHS
NHS Foundation Trust

Data Protection Act 1998

Notification & Data Mapping Form

with guidance for completion

(see page 3 for initial information)

Completed forms should be returned to the
Information Governance, Caldicott & SIRO Support Manager
Department for Information Governance, Caldicott & SIRO Support
Sheffield Teaching Hospitals NHS Foundation Trust
Weston Park Hospital
Whitham Road, Sheffield. S10 2SJ

DOCUMENT CONTROL

Reference Number	**Version**	**Status**	**Executive Leads**	**Author**	
190	5.0	Current	SIRO, Caldicott Guardian	Peter Wilson	
Approval Body	Information Governance Committee			**Date Approved**	18/02/2011
Ratified By	TEG			**Date Ratified**	02/03/2011
Date Issued	15/08/11			**Review Date**	31/03/2013
Contact for Review:	Peter Wilson, Information Governance, Caldicott & SIRO Support Manager Department for Information Governance, Caldicott & SIRO Support				

Data Notification & Dating Mapping Form - Associated Documentation

Policies:

Sheffield Teaching Hospitals Trust controlled documents:

17. Email Policy
18 Internet Acceptable Use Policy
27. Data Protection Policy
29. Information Security Policy
42 Information Governance Management Framework
69. Password Policy
170. Safehaven Policy
165 Mandated Procedures for the Transfer of PID and other Sensitive or Confidential Information
197. Information Risk Management Policy

Legal framework:

Data Protection Act 1998
Data Protection (Processing of Sensitive Personal Data) (Elected Representatives) Order 2002
Privacy and Electronic Communications Regulations 2003,
Computer Misuse Act 1990
Freedom of Information Act 2000,
Environmental Information Regulations 2004
Human Rights Act 1998,
Health & Social Care Act 2006
Criminal Justice and Immigration Act 2008

Codes of Conduct and Practice:

Sheffield Teaching Hospitals Trust controlled documents:

36. Confidentiality – Staff Code of Conduct
70. Code of Practice in the Use of Passwords
71. Code of Practice for Storing and Managing Information on Network and Local Computer Drives
72. Code of Practice in the Use of Email
165. Mandated Procedures for the Transfer of PID or other Sensitive or Confidential Information
201. Code of Practice in the Use of Trust Issued USB Sticks

Staff Conditions of Contract

IG Local Controlled Document

I/09000/35/1 Information Asset Owners ~ Responsibilities and Training

External documentation

Records Management: NHS Code of Practice, parts 1 & 2: April 2006
Section 46, Freedom of Information Act 2000, Code of Practice for the Management of Records.
The NHS Confidentiality Code of Practice (Guidelines on the use and
protection of patient information, November 2005)

Version Control

Version	Date Issued	Brief Summary of Changes	Owners name
2.0	11/06/04	Development and claification to layout	Peter Wilson
2.5	02/08/04	Minor amendments to layout	Peter Wilson
3.0	15/08/08	EU countrylist amended	Peter Wilson
4.1	21/08/08	Major redesign: information security aspects added Appendix A:Laptop audit & Appendix B: Data mapping added	Peter Wilson
4.2	11/11/08	Database definition added. Forms delineated by alphabetical identifier. Research Dept Tel. No updated	Peter Wilson
4.3	02/02/09	Minor change to Appendix A. Main document unchanged	Peter Wilson
4.4	21/08/09	Minor change to Appendix A. Main document unchanged	Peter Wilson
4.5	09/02/10	Minor change to Appendix B. Main document unchanged Appendix C: Application for a USB Stick added	Peter Wilson
5.0	15/02/11	Document reviewed, reformatted into new layout. Executive summary added, minor updates to associated documentation details. Form A modified to include asset owners and administrators, rather than system owners and managers. Form 'cleaned up' to ease completion and clarity: no material changes	Peter Wilson

Executive Summary

Data Notification & Dating Mapping Form

Document objectives:
To register all databases and associated Information Assets held within the Trust as per the DPA notification to the ICO and the requirements of the Information Governance Assurance Framework. To identify, map and assess associated risks to the data through their storage, processing and transfer

Group/Persons Consulted:
Research Department, data holders, data processors, data transfer recipients, IAOs, SIRO, Information Governance Committee (IGC), Department for Information Governance, Caldicott & SIRO Support (IGCS)

Monitoring Arrangements and Indicators:
Notification and return of the completed forms. Identification of information assets, systems and databases with their relevant process and mapping. Audit of recorded data holders, IAO reports to SIRO

Training Implications
8.112 Information Governance Training Tool (IGTT) online. Specialist training and support facilitated by IGCS where necessary

Equality Impact Assessment
Completed and signed off

Resource Implications
Part of the Trust approach to the confidentiality, integrity and availability of all data. This should be integrated into working practices as standard

Intended Recipients
All staff handling Information Assets, databases and data flows: IAOs and IAAs

Who should:
Be **aware** of the document and where to access it
The SIRO, the IAOs, the Trust Board

Understand the document
Research Department, IAOS and IAAs, staff working with Information Assets and/or staff who facilitate systems that hold or support Information Assets. IGCS who maintain the Information Asset Register

Have a **good working knowledge** of the document
Research Department, IAOs, IAAs and the SIRO,staff of IGCS

Completing the Data Notification and Mapping Form

There are two ways of completing the form

- Print out and complete by hand, or
- electronically

When completing manually, sign off and keep a hard copy for your records: send the completed form through to the Department of Information Governance, Caldicott & SIRO Support. (IGCS)
To complete electronically:

- open the file on your computer
- check that light blue shading is showing; these are editable fields in the form.
- complete the editable fields where relevant (text or box using an “X” to select)
- To save the completed form **DO NOT** use “File”, and “Save” because it doesn’t, instead
- Use “File” and “Print”
- When the Print dialogue box opens click in the the “Printer, Name” field
- From that drop down menu choose “Adobe PDF”
- Click on “OK” and a dialogue box will open showing where the file will be saved and giving the file a default title. (The existing name of the document).
- Amend the save location if required.
- Amend the default title either to the name of the database being registered or the STH Number.
- Click on “Save” and the completed document will become a new PDF with your information saved.
- IGCS will accept electronic submission without signature if from a valid related email address.

NOTE: the new document cannot be electronically amended, so ensure all the information added to the original is correct before carrying out this process. The original data entry pdf cannot be saved unless you have advanced versions of Adobe Acrobat Professional v.9 or above.
The blue shading in the original document does not print out when manually completing, and does not transfer when the original is resaved as a new pdf

Data Notification & Dating Mapping Form

All forms labelled A to F, and Appendices A & B should be completed where relevant.

Note: Research project finance forms will not be signed off by the Trust Data Controller unless accompanied by a completed copy of this form.

Contents

Database definition - what is a database?

In the broadest sense, a database is anything that stores data. A phone book, for instance, could be considered a database as it stores related pieces of information such as name and phone number. However, in the world of computers, a database usually refers to a collection of related pieces of information stored electronically. Aside from the ability to store data, a database also provides a way for other computer programs to quickly retrieve and update desired pieces of data.

The central concept of a database is that of a collection of records, or pieces of knowledge stored or collected electronically or in hard copy (folders, drawers, and filing cabinets). Typically, for a given database, there is a structural description of the type of facts held in that database: this description is known as a schema. The schema describes the objects that are represented in the database, and the relationships among them. There are a number of different ways of organizing a schema, that is, of modelling the database structure: these are known as database models (or data models).

The most common model for a database is a relational model. These databases are organized by fields, records, and tables. A field is a single piece of information; a record is one complete set of fields; and a table is a collection of records. With this simple model, just about any relationship between any collection of data can be represented

A. Data Protection Notification Form

Please indicate box selection using an "X"

STH Number

Sheffield Teaching Hospitals NHS
NHS Foundation Trust

Department for Information Governance, Caldicott & SIRO Support

D/04000/17/1 DPA Notification & Data Mapping Form v 5.0

Notes for Guidance on Page 6

1.0 Name/Subject of the System/Database

2.0 Asset Owner | 3.0 Position/JobTitle

4.0 Asset Administrator | 5.0 Department

6.0 Manual/Electronic System **M** ☐ **E** ☐ 7.0 Implementation Date

8.0 Location of Database: Room No. | Building | Hospital

9.0 Correspondence Address

Post Code | 10.0 Head of Department

11.0 Asset Owner Tel. No. & E-mail address | @

12.0 Asset Administrator Tel. No. & E-mail address (if not 11) | @

13.0 Have Informatics been involved in setting up the database? **Y** ☐ **N** ☐

14.0 Is the database used for: a) Business Management? **Y** ☐ **N** ☐ b) Research? **Y** ☐ **N** ☐ c) Clinical Management? **Y** ☐ **N** ☐

15.0 If 14b is Yes, has the project been registered with the Research Department? **Y** ☐ **N** ☐

16.0 If 14c is Yes, will the database be used to support clinical decision making? **Y** ☐ **N** ☐

17.0 If 16 is Yes, please give details:

18.0 Security arrangements for risk assessment purposes. *Tick all relevant boxes*

The database is held/stored on:

a) Trust Network Data Store ☐
b) Trust PC ☐
c) Trust Laptop ☐
d) Other Laptop ☐
e) University electronic systems ☐
f) Portable Electronic Storage ☐
g) PDA or similar ☐

19.0 Database disposal date

Month/year - if known

Storage of a manual database is in:

h) Trust secure filing cabinet ☐
i) Trust secure locked room ☐
j) Trust safe ☐
k) Other ☐

If you have ticked **any** of boxes **18b** to **18g,** or box **18k**, either of boxes **18l** and **18m** you **must** complete the **Risk Shee**t on page 4, and any other registrations necessary

Data movement

l) Are data electronically transferred to external (non STH) data storage? **Y** ☐ **N** ☐

m) Are the hard copy data ever manually transported off campus? **Y** ☐ **N** ☐

By signing you certify compliance with the Trust's Notification to the Information Commissioner under the Data Protection Act 1998, the Caldicott Principles and the Information Governance Assurance Framework.

Signature..... Date:.....

Print name..... Tel:.....

When complete go to Page 7

Notes for Guidance on Page 6

Data Protection Notification Form - Notes for Guidance

1.0 Name/Subject of the System/Database

Please enter an identifying name or subject which is specific to the database content

2.0 Asset Owner (originally System Owner)

The Owner of the Information Asset or the database initiator: in Research the person who will use the data, ie the PI: for IT corporate and clinical systems the Asset Owner for purposes of risk management & security

3.0 Position/Job Title

This field is mandatory

4.0 Asset Administrator (originally System Manager)

The person who is responsible for data entry. In Research this could be the same person as the Asset Owner, large Information Assets will have a separate Administrator(s)

5.0 Department

Full Department name, please

6.0 Manual/Electronic

Please tick the box

7.0 Implementation Date

Please show the proposed operational date for a newly developed database. where the form is completed retrospectively, enter the original start date.

8.0 Location of Database

This is important in risk assessment and information governance. Please complete in full.

9.0 Correspondence Address

A crucial piece of information. This should be the address fo r all requests for a search under the Data Protection Act 1998. This will usually be the address of the Information Asset/System Owner.

10.0 Head of Department

A name is required here, not a signature.

11.0 & 12.0 Asset/System Owner/Manager/Administrator Tel. No. & Email address

Please complete in full, vital if we need to contact you urgently.

13.0 Have Informatics been involved in the setting up of the database?

Unless Informatics have been informed of, or involved with the development of the database, no support will be forthcoming in the event of application error or malfunction attributable to the database.

14.0 Is the database used for a) Business Management? b) Research c)Clinical Management?

Please tick the appropriate box

15.0 If 14b is Yes, has the project been registered with the Research Department?

It is Trust policy that all research projects be formally approved by the STH Research Department prior to their start up. Please contact the Research Department on 0114 2265935 for further details.

16.0 If 14c is Yes, will the database be used to support clinical decision making?

Please tick the appropriate box

17.0 If 16 is Yes, please give details

Please address fully.

18.0 Security and data mapping arrangements

Sections 18a to 18l address information security and enable the Department for Information Governan ce, Caldicott & SIRO Support to assess risk and vulnerability. Full completion of this Section and, where necessary, the Risk Sheet on page 4 of this document, would greatly assist in ensuring that the Trust meets its mandated requirements under the Information Governance Assurance Framework (IGAF).

19.0 Database disposal date

If the database has a specific life cycle, please give an expected date of withdrawal from use

B. Risk Assessment Sheet - Security and Confidentiality

To be completed when any of Sections 18b to 18m on page 5 have been selected.

Please indicate box selection using an "X"

1. Does the database contain any personally identifiable, confidential or sensitive personal data? YES ☐ NO ☐

2. If you ticked **Section 18b**, is the PC

18b Networked? YES ☐ NO ☐ Password Protected? YES ☐ NO ☐

Encrypted? YES ☐ NO ☐ DON'T KNOW ☐

3. If you ticked **Section 18c**, is the Trust Laptop

18c Networked? YES ☐ NO ☐ Password Protected? YES ☐ NO ☐

Encrypted? YES ☐ NO ☐ DON'T KNOW ☐

Registered under the Trust Laptop Audit? YES ☐ NO ☐ DON'T KNOW ☐

If the Laptop is not registered please complete the form in Appendix A of this document.

4. If you ticked **Section 18d**, is the Other Laptop

18d Networked? YES ☐ NO ☐ Password Protected? YES ☐ NO ☐

Encrypted? YES ☐ NO ☐ DON'T KNOW ☐

Configured by the Trust IT Department? YES ☐ NO ☐ DON'T KNOW ☐

Registered under the Trust Laptop Audit? YES ☐ NO ☐ DON'T KNOW ☐

If the Laptop is not registered please complete the form in Appendix A of this document.

5. If you ticked **Section 18e**, university electronic system

18e Was the patient informed of, and consented to this storage? YES ☐ NO ☐

6. If you ticked **Section 18f**, portable electronic storage, is it

18f Encrypted? YES ☐ NO ☐ DON'T KNOW ☐

Password Protected? YES ☐ NO ☐

7. If you ticked **Section 18g**, PDA or similar, is it

18g Encrypted? YES ☐ NO ☐ DON'T KNOW ☐

Password Protected? YES ☐ NO ☐

Dockable with Trust and other IT systems? YES ☐ NO ☐ DON'T KNOW ☐

8. If you ticked **Section 18k**, other, please describe your security arrangements

18k .....

9. If you ticked **Section 18l, Yes** are data electronically transferred to external (non STH) data storage?

18l Has the patient consented to this data flow? YES ☐ NO ☐

Has the data flow been mapped and registered? YES ☐ NO ☐

If the data flow has not been registered please complete the form in Appendix B of this document.

10. If you ticked **Section 18m, Yes**, are the hard copy data ever manually transported off campus?

18m Has the patient consented to this data flow? YES ☐ NO ☐

What security measures are used to protect the data? .....

Has the data flow been mapped and registered? YES ☐ NO ☐

If the data flow has not been registered please complete the form in Appendix B of this document.

C. Purposes

To complete, please type an "X" in the appropriate box. If a purpose is selected which is marked with an asterisk, provide further details of the business activity in the box below to clarify the standard purpose activity

- ☐ Staff Administration
- ☐ Acounts & Records
- ☐ Accounting & auditing
- ☐ Administration of membership records
- ☐ Benefits, grants & loans administration*
- ☐ Consultancy and advisory services*
- ☐ Crime prevention & prosecution of offenders
- ☐ Education
- ☐ Fundraising
- ☐ Health administration and services
- ☐ Information and databank administration
- ☐ Legal Services
- ☐ Licensing and registration
- ☐ Pastoral care
- ☐ Pensions administration
- ☐ Processing for "Not for Profit" organisations
- ☐ Property management
- ☐ Provision of financial services and advice
- ☐ Public health
- ☐ Research*

Additional information

Purposes - Notes for Guidance

In this section you will describe the purpose for which personal data are to be held or used. Wherever possible, these predefined purposes must be used. However, if none of these apply you may use your own words to describe your purpose. If you do, the standard text description will appear in your register entry. Please note that although each description includes typical activities which may be associated with the purpose, these are example activities only. No implication that all of them are carried out, nor that they illustrate all the possible activities involved.

You may find it helpful to relate the purpose to a specific part or parts of the Trust or to a particular activity, where these are of major significance. For certain purposes you are required to provide further details of the activity to clarify the standard purpose description. These are indicated by an asterisk.

Please note, if the data are used for more than one purpose, a separate Data Protection Notification form must be used for each purpose.

STANDARD BUSINESS PURPOSES

Staff administration

Appointments or removals, pay, discipline, superannuation, work management or other personnel matters in relation to the staff of the data controller.

Accounts and records

Keeping accounts relating to any business or other activity carried on by the data controller, or deciding whether to accept any person as a customer or supplier, or keeping records of purchase sales or other transactions for the purpose of ensuring that the requisite payments and deliveries are made or services provided by him or to him in respect of those transactions, or for the purpose of making financial or management forecasts to assist him in the conduct of any such business or activity.

Notes for Guidance continues on page 9

When complete go to Page 10 →

OTHER PURPOSES

Accounting and auditing
The provision of accounting and related services; the provision of an audit wherever such an audit is required by Statute.

Administration of membership records
The administration of membership records.

Benefits, grants and loans administration
*The administration of welfare and other benefits. Please indicate the type(s) of benefit you are administering **

Consultancy and advisory services
*Giving advice or rendering professional services. The provision of services of an advisory, consultancy or intermediary nature. Please indicate the nature of the services which you provide.**

Crime prevention and prosecution of offenders
Crime prevention and detection, and the apprehension and prosecution of offenders.

Education
The provision of education or training as a primary function or as a business activity.

Health administration and services
The provision and administration of patient care.

Information and databank administration
Maintenance of information or databanks as a reference tool or general resource. This includes catalogues, lists, directories and bibliographic databases.

Legal services
The provision of legal services, including advising and acting on behalf of clients.

Licensing and registration
The administration of licensing or maintenance of official registers.

Pastoral care
The administration of pastoral care by a vicar or other minister of religion.

Pension administration
The administration of funded pensions or superannuation schemes. Data controllers using this purpose will usually be the trustees of pension funds.

Processing for 'not for profit' organisations
Establishing or maintaining membership of or support for a body or association which is not established or conducted for profit, or providing or administering activities for individuals who are either members of the body or association or have regular contact with it.

Property management
The management and administration of land, property and residential property and the estate management of other organisations.

Provision of financial services and advice
The provision of services as an intermediary in respect of any financial transactions including mortgage and insurance broking.

Public Health
The provision of and support of all areas concerned with public health.

Research
*Research in any field, including health, scientific, technical, lifestyle or marketing research. Please indicate the nature of the research undertaken. **

D. Data Subjects

The standard data subject descriptions are listed on the form. When selecting data subject types from the list you may find it helpful to consider whether you can best describe the data subject in terms of his primary relationship with you the data user. In other words, is he your employee or your customer? There is likely to be some overlap between types, for example some of your customers could well be students or self-employed. There is no need to type an "X" in the boxes other than the primary ones, unless by doing so you add significantly to the description.

You may add extra descriptions in text if you wish, but do not do this unless it is absolutely necessary.

To complete, please select the appropriate box, and either of the CU, PA, or PO boxes
Where CU = Current, PA = Past, PO= Potential

The following is a list of standard descriptions of data subjects. A data subject is an individual about whom personal data is held

	Code	Standard Descriptions	C	PA	P
☐	S100	Staff including volunteers, agents, temporary and casual workers	☐	☐	☐
☐	S101	Customers and clients	☐	☐	☐
☐	S102	Suppliers	☐	☐	☐
☐	S103	Members or supporters	☐	☐	☐
☐	S104	Complainants, correspondents and enquirers	☐	☐	☐
☐	S105	Relatives, guardians and associates of the data subject	☐	☐	☐
☐	S106	Advisers, consultants and other professional experts	☐	☐	☐
☐	S107	Patients (data or tissue)	☐	☐	☐
☐	S108	Students and pupils	☐	☐	☐
☐	S109	Offenders and suspected offenders	☐	☐	☐
☐	S900	.....	☐	☐	☐
☐	S901	.....	☐	☐	☐
☐	S902	.....	☐	☐	☐
☐	S903	.....	☐	☐	☐
☐	S904	.....	☐	☐	☐
☐	S905	.....	☐	☐	☐

When complete go to Page 11 ➡

E. Data Classes

	Code	Standard Descriptions
☐	C200	Personal details
☐	C201	Family, lifestyle and social circumstances
☐	C202	Education and training details
☐	C203	Employment details
☐	C204	Financial details
☐	C205	Goods or services provided
☐	C206	Racial or ethnic origin
☐	C207	Political opinions
☐	C208	Religious or other beliefs of a similar nature
☐	C209	Trade Union membership
☐	C210	Physical or mental health or condition
☐	C211	Sexual Life
☐	C212	Offences (including alleged offences)
☐	C213	Criminal proceedings, outcomes and sentences
☐	C214	Diagnosis
☐	C215	Mortality Status
☐	C216	Health outcome measures or morbidity
☐	C900	.....
☐	C901	.....
☐	C902	.....
☐	C903	.....
☐	C904	.....
☐	C905	.....

Notes for Guidance are on Page 12

When complete go to Page 13 →

Data Classes - Notes for Guidance

Standard data class descriptions are also listed here. Please note that the data items are examples only. The list is not exhaustive and the fact that you have ticked a particular Data Class does not necessarily mean that you are holding all, or indeed any, of the example data items listed against that Class. Also, there is no implication that all the Data Classes are held for all data subjects.

Nevertheless, you may feel that certain Data Classes are particularly sensitive and that the standard descriptions need some refinement. You can do this in free text if you wish. You can also add extra descriptions in text if you are holding data not covered by any of the standard descriptions.

Please remember in completing this section that you are describing data to be held for the purpose described.

Data Classes

We provide the following list of standard descriptions of data classes. Data classes are the types of personal data which are being or which are to be processed.

C200 - Personal details

Included in this category are classes of data which identify the data subject and their personal characteristics. Examples are names, addresses, contact details, age, sex, date of birth, physical descriptions, identifiers issued by public bodies, e.g. NI number.

C201 - Family, lifestyle and social circumstances

Included in this category are any matters relating to the family of the data subject and the data subject's lifestyle and social circumstances. Examples are details about current marriage and partnerships and marital history, details of family and other household members, habits, housing, travel details, leisure activities, membership of charitable or voluntary organisations.

C202 - Education and training details

Included in this category are any matters which relate to the education and any professional training of the data subject. Examples are academic records, qualifications, skills, training records, professional expertise, student and pupil records.

C203 - Employment Details

Included in this category are any matters relating to the employment of the data subject. Examples are employment and career history, recruitment and termination details, attendance record, health and safety records, performance appraisals, training records, security records.

C204 - Financial details

Included in this category are any matters relating to the financial affairs of the data subject. Examples are income, salary, assets and investments, payments, credit-worthiness, loans, benefits, grants, insurance details, pension information.

C205 - Goods or services provided

Included in this category are classes of data relating to goods and services which have been provided. Examples are details of the goods or services supplied, licences issued, agreements and contracts.

The examples given are not an exhaustive list of what may be included in each category.

Sensitive Data

The following categories of data have been designated as sensitive personal data. If you process the following types of data they must be specified in your notification.

C206 - Racial or ethnic origin
C207 - Political opinions
C208 - Religious or other beliefs of a similar nature
C209 - Trade Union membership
C210 - Physical or mental health or condition
C211 - Sexual Life
C212 - Offences (including alleged offences)
C213 - Criminal proceedings, outcomes and sentences
C900 - C905 Free text boxes

F. Recipients

In this section, you are asked to describe the recipients whom you intend or potentially may wish to disclose data. It does not include any person to whom the data controller may be required, by law, to disclose in any particular case, for example, if required by the Police under a Warrant.*
**Sheffield Teaching Hospitals NHS FoundationTrust (The Trust) is the Data Controller, System Owners and Managers are classed as Data Processors*

To complete, please type an "X" in the appropriate box(es).

	Code	Standard Descriptions
☐	R400	Data subjects themselves
☐	R401	Relatives, guardians or other persons associated with the data subject
☐	R402	Current, past or prospective employers of the data subject
☐	R403	Healthcare, social and welfare advisers or practitioners
☐	R404	Education, training establishments and examining bodies
☐	R405	Business associates and other professional advisers
☐	R406	Employees and agents of the data controller
☐	R407	Other companies in the same group as the data controller
☐	R408	Suppliers, providers of goods or services
☐	R409	Persons making an enquiry or complaint
☐	R410	Financial organisations and advisers
☐	R411	Credit reference agencies
☐	R412	Debt collection and tracing agencies
☐	R413	Survey and research organisations
☐	R414	Traders in personal data
☐	R415	Trade, employer associations and professional bodies
☐	R416	Police Forces
☐	R417	Private Investigators
☐	R418	Local Government
☐	R419	Central Government
☐	R420	Voluntary and charitable organisations
☐	R421	Political organisations
☐	R422	Religious organisations
☐	R423	Ombudsmen and regulatory authorities
☐	R424	The media
☐	R425	Data processors
☐	R428	Courts and Tribunals
☐	R900	.....
☐	R901	.....
☐	R902	.....
☐	R903	.....
☐	R904	.....
☐	R905	.....

Note: If disclosures are ticked please enter further details on page 15 of persons/organisations to whom data are disclosed. This will assist in risk assessment and process/data flow mapping

When complete go to Page 15

F. Recipients (continued)

If disclosures were ticked on page 12, please enter further details of persons/organisations to whom data are disclosed.

Name/Status/Function **Organisation/Department**

When complete go to Page 15

G. Transfers of Personal Data

*In this section, you are asked to indicate whether personal data are transferred outside the United Kingdom or outside the European Economic Area (EEA).**

The choices are:-

"None outside the UK
"None outside the EEA"
"Worldwide"

The UK comprises England, Scotland, Wales and Northern Ireland

Name individual countries outside the EEA (if there are more than ten countries indicate 'worldwide').

A transfer is not defined in the Act. However, the ordinary meaning of the word is transmission from one location, person etc. to another. This will include posting information on a website which can be accessed from overseas. In these circumstances, it would be appropriate to indicate 'worldwide'.

The countries in the EEA are:- Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece,Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Rumania, Slovak Republic, Slovenia, Spain, Sweden, United Kingdom, Iceland, Liechtenstein*, Norway*.*

** These countries are in the EEA, but are not members of the European Union*

Choices

☐ **1** **None outside the UK**

☐ **2** **None outside the EEA**

☐ **3** **Worldwide**

☐ **4** **Named individual countries outside the EEA****

Country 1 .....
Country 2 .....
Country 3 .....
Country 4 .....
Country 5 .....
Country 6 .....
Country 7 .....
Country 8 .....
Country 9 .....
Country 10 .....

* * If there are more than 10 countries indicate "Worldwide"

Notification & Data Mapping Form

This page intentionally blank ~
Appendices follow

Appendix A

Information Governance Assurance

Laptop Audit Manual Reply Form

Sheffield Teaching Hospitals NHS
NHS Foundation Trust

Department for Information Governance, Caldicott & SIRO Support

Please tick the appropriate box and complete the free .text areas where necessary.
For additional information read the notes on the reverse of this form.

1. Complete if you use a laptop for any work or research purpose at STHFT

Full name: | Email address

Department/Directorate

Department/Directorate address

Tel. No.

2. Is your laptop owned, or configured by STHFT? YES ☐ NO ☐

If YES, please enter the audit number ☐

3. If not STHFT, select the owner

3a. Personal/Family ☐ | 3b. University of Sheffield ☐

3c. Sheffield Hallam University ☐ | 3d. Professional Body ☐

3e. Other Organisation ☐

3f. Manufacturer ☐ | 3g Model Number ☐

3h. Serial Number ☐

3i. Operating System: Windows 2000 ☐ | Windows XP ☐ | Windows Vista/7 ☐

Mac OS X ☐ | Linux based ☐ | Other O/S ☐

4. Laptop's usual location: Office (only) ☐ | Home (only) ☐ | Office & Home ☐

Other ☐

If other, please specify:

5. Is the laptop used solely by you? YES ☐ NO ☐

If NO, please list all other users

6. Do you connect to the Trust's network (for the intranet, or systems)? YES ☐ NO ☐

7. Do you connect to any other network? YES ☐ NO ☐

If YES, please provide details:

8. Is Person Identifiiable Data (PID) stored on the laptop? YES ☐ NO ☐

If YES, please provide details

9. Is the laptop password protected (does every user require a password)? YES ☐ NO ☐

10. Is encryption software installed on the laptop? YES ☐ NO ☐ DON'T KNOW ☐

If YES, please give details of the encryption software installed

Information Governance Assurance

Laptop Audit Manual
Reply Form

Guide to Audit Questions

More detailed information about the audit questions is given below, some information needs to be collected before you complete the audit form e.g. computer number, laptop model number, serial number etc. It is therefore recommended that you print off this email as a reference document before you complete the on-line audit form.

(1) States the target audience for the form

(2) Answer YES if the laptop was purchased by the Trust for your use, the computer audit number is usually on a blue and silver metallic label headed STH IT Support Services or on an attached label, enter all audit number digits.

(3) If the laptop was not purchased by the Trust record who it was purchased by and detail the manufacturer, model number, serial number (usually on a label on the base of themachine) and the operating system (this is displayed when the machine is first switched on).

(4) Record where the laptop is used for the majority of the time.

(5) Please record the names of other staff who use the laptop if it is a shared machine.

(6) If the laptop is connected to the Trust's network (for the Intranet or other systems e.g. PAS, InfoFlex, PROTON etc) by cable or a wireless link answer YES.

(7) If you connect the laptop to any other networks answer YES and give details e.g. University network, Home internet service provider (ISP) etc.

(8) Is Person Identifiable Data (PID) or other Sensitive or Confidential Information stored on the laptop. If the answer is YES please provide brief details.
(PID is defined as any patient or staff information which would enable that person's identity to be established by one means or another. Sensitive or confidential information is regarded as information which if lost or misdirected could impact adversely on individuals, the organisation or the wider community. In addition to personal and clinical information confidential information could also include financial information, commercial information and details of any security arrangements).

(9) Answer YES if you have set up a personal password to enable you to access the laptop, this is in addition to the Username and Password you use to connect to the Trust network.

(10) Answer YES if you have any encryption software already installed or activated on the laptop e.g. TrueCrypt, Safeboot etc.

If you are unsure about any question contact the Department for Information Governance & Caldicott & SIRO Support on Ext 65151 or email infogov@sth.nhs.uk for advice before you complete the audit form.

Appendix B

Ref: IGA .....

Information Governance Assurance

Data Mapping & Processing Notification Form

To be used to register data mapping and information flows of Person Identifiable Data (PID), sensitive and confidential information throughout the Trust.

Sheffield Teaching Hospitals NHS
NHS Foundation Trust

Department for
Information Govenance & Caldicott Support
Floor 5, Weston Park Hospital
Whitham Road, Sheffield. S10 2SJ
Tel: 0114-2265151 Fax: 0114-2265152
Email: infogov@sth.nhs.uk

Return to the above address on completion

1. Name:	2. Designation:
3. Department:	4. Tel/bleep/email:

5.Name of database/dataflow:

6. Purpose and content:

7. Is the data anonymised or pseudonymised? YES ☐ NO ☐

8. Data classes held: *Where applicable. See notes overleaf*

1. ..... 4. .....
2. ..... 5. .....
3. ..... 6. .....

9. Data Protection Registration Number *(where applicable)*

10. STH Research Study Reference Number *(where applicable)*

11. Audit Study Name *(where applicable)*

12. Is the data transferred to other areas and other users? YES ☐ NO ☐

13. If yes, are the transfers: a) Internal? ☐ b) External? ☐ c) Internal and External? ☐

14. If external, name recipient, location & country

15. What is the purpose of the transfer?

16. Are the transfers: a) Electronic? ☐ b) paper/hard copy? ☐

17. If electronic, describe the delivery method and the media used

18. If the data transfer is electronic and external is it encrypted? YES ☐ NO ☐

19. If YES, please give details of the encryption software installed

20. If paper/hard copy, how is it sent, tracked, secured and its receipt acknowledged?

21. State volume and frequency of data transfer

22. Has the data transfer/storage been risked assessed? YES ☐ NO ☐

23. If YES, who carried out the risk assessment? ..... When? d d m m y y

24. Has the transfer been approved by Information Governance? YES ☐ NO ☐

25. If YES, when? d d m m y y

26. Signed .....

27. Print Name .....

Information Governance use only:
Process registered, assessed & recorded
Signed .....
Date .....

Data Classes

Code	Standard Descriptions
C200	Personal details
C201	Family, lifestyle and social circumstances
C202	Education and training details
C203	Employment details
C204	Financial details
C205	Goods or services provided
C206	Racial or ethnic origin
C207	Political opinions
C208	Religious or other beliefs of a similar nature
C209	Trade Union membership
C210	Physical or mental health or condition
C211	Sexual Life
C212	Offences (including alleged offences)
C213	Criminal proceedings, outcomes and sentences
C214	Diagnosis
C215	Mortality Status
C216	Health outcome measures or morbidity

Data Classes
This is a list of standard descriptions of data classes.
Data classes are the types of personal data which are being or which are to be processed.

Confidential Data
C200 - Personal details
Included in this category are classes of data which identify the data subject and their personal characteristics. Examples are names, addresses, contact details, age, sex, date of birth, physical descriptions, identifiers issued by public bodies, e.g. NI number.

C201 - Family, lifestyle and social circumstances
Included in this category are any matters relating to the family of the data subject and the data subject's lifestyle and social circumstances. Examples are details about current marriage and partnerships and marital history, details of family and other household members, habits, housing, travel details, leisure activities, membership of charitable or voluntary organisations.

C202 - Education and training details
Included in this category are any matters which relate to the education and any professional training of the data subject. Examples are academic records, qualifications, skills, training records, professional expertise, student and pupil records.

C203 - Employment Details
Included in this category are any matters relating to the employment of the data subject. Examples are employment and career history, recruitment and termination details, attendance record, health and safety records, performance appraisals, training records, security records.

C204 - Financial details
Included in this category are any matters relating to the financial affairs of the data subject. Examples are income, salary, assets and investments, payments, credit-worthiness, loans, benefits, grants, insurance details, pension information.

C205 - Goods or services provided
Included in this category are classes of data relating to goods and services which have been provided. Examples are details of the goods or services supplied, licences issued, agreements and contracts.

The examples given are not an exhaustive list of what may be included in each category.

Confidential & Sensitive Data
The following categories of data have been designated as sensitive personal data.
If you process the following types of data they must be specified in your notification.

C206	-	Racial or ethnic origin
C207	-	Political opinions
C208	-	Religious or other beliefs of a similar nature
C209	-	Trade Union membership
C210	-	Physical or mental health or condition
C211	-	Sexual Life
C212	-	Offences (including alleged offences)
C213	-	Criminal proceedings, outcomes and sentences
C214	-	C216 Health related

! NOTE: If the data processed or mapped comes from, or is transferred to, any form of manual or electronic Trust database, the database(s) must be registered with Information Governance. This is a legal requirement of the Data Protection Act 1998. To register complete a DP Notification Form available from Information Governance.

Appendix C

Ref: RPM IG .....

Sheffield Teaching Hospitals NHS
NHS Foundation Trust

Department for
Information Governance, Caldicott & SIRO Support-
Floor 5, Weston Park Hospital
Whitham Road, Sheffield. S10 2SJ
Tel: 0114-2265151 Fax: 0114-2265152
Email: infogov@sth.nhs.uk

Return to the above address on completion

Information Governance Assurance

Registration of removable and portable electronic storage media used for the transfer of Trust Personal Identifiable Data (PID), Sensitive & Confidential Information

Use this form for all types removable & portable storage devices, ***except*** *Trust issued USB sticks and laptops.*
Only *encrypted USB sticks registered and issued by the Trust, should be used for PID.*
Laptops ***must*** *be registered separately*

Note: anonymised and pseudonymised data is not PID: see overleaf

1. Name:

2. Designation:

3. Department:

4. Tel/bleep/email:

5. Media type, make and model

6. Is it a) Trust issued? YES ☐ NO ☐ b) Personal? YES ☐ NO ☐

7. Is it a) Password protected? YES ☐ NO ☐ b) Encrypted? YES ☐ NO ☐

8. If 7b) is yes, is the encryption security level? a) 128bit AES ☐ b) 256bit AES ☐

9. Details of PID regularly stored on or transferred using the device *(list all that apply)*

10. Have the data storage/transfers been risked assessed? YES ☐ NO ☐

11. If 10 is yes, who risk assessed the data storage/transfers?

12. Have the data flows/transfers been approved? YES ☐ NO ☐

13. If 12 is yes, who approved the data flows?

14. Have all the data flows/transfers been mapped and registered with IG? YES ☐ NO ☐

Please note: it is Trust policy that all removable or portable electronic storage media that contain PID and other sensitive and confidential information must be encrypted, and the data mapped and registered. All external electronic data flows by e-mail that contain PID must be encrypted, data mapped and registered, unless sent by NHS-mail to another NHS-mail account when they should be data mapped and registered. Electronic data flows within the Trust network, ie to other internal departments and via internal sth.nhs.uk e-mail to an sth.nhs.uk e-mail address need not be registered. External hard copy data flows of PID should be mapped and registered even if the flow is from campus to campus.
See related Information Governance policies and procedures for further information.

15. If 14 is yes, please supply Data Mapping reference number(s) where known.

IGA ..... IGA ..... IGA ..... IGA .....
IGA ..... IGA ..... IGA ..... IGA .....
Continue on a separate sheet if necessary

16. If 14 is no, please complete a Data Mapping Notification Form for each data flow or transfer

Please note: failure to provide details of existing and proposed PID data flows and transfers using the Notification & Data Mapping Form breaches Trust policies and procedures and could lead to disciplinary action.

I confirm Registration of the above device and confirm all data flows are mapped and encryption standards engaged

Signed .....

Dated d d m m y y

Information Governance use only:

Form checked & validated by .....

Signed .....

Data entry d d m m y y

Removable and Portable Electronic Storage Media Definitions

Removable and portable electronic storage media devices may include, but are not limited to palmtops, Blackberrys, laptops, net books, mobile phones, digital cameras, flash drives (including compactflash and USB pen drives), portable hard disk drives, floppy diskettes, CDs, DVDs, HD-DVDs.

Due to the portability of these devices, care needs to be taken to ensure their physical security to prevent potential compromise through loss or theft.

Refer to Trust policies and procedures relating to hardware and physical security, encryption and password protection, data and information transfer protocols. Failure to protect PID, sensitive and confidential information may be classed as a breach of Trust policy and could result in disciplinery action.

Anonymised and Pseudonymised Data Definitions

Anonymised data

Data concerning an individual from which the identity of the individual cannot be determined. The second Caldicott principle is that patient identifiable information should not be used unless absolutely necessary: use anonymised data instead.

In practice, anonymised data should exclude the name, address and full post code, and any other information which when combined with other information likely to be held by or available to the recipent could allow the individual to be identified.

Unique identifiers such as hospital or NHS number should also be excluded if there is any possibility that any recipient of the data has access to the 'key' to that identifier and could thereby trace the identity of the individual.See pseudonymisation, below..

Anonymised and aggregated information can only be used for justified purposes. Staff must ensure that individuals cannot be identified from the information

Pseudonymised Data

The European Commission on Data Protection (DP) has defined pseudonymised data as non-personal data and not subject to the Data Protection Directive in certain instances.

In its “Opinion 4/2007 on the concept of personal data”, the European Commission Article 29 Data Protection Working Party (WP) clarified the notion of "personal data" thus enhancing legal certainty through the uniform interpretation of the EC Directive 95/46/EC. The document describes the following conditions necessary to consider pseudonymised data as non-personal data and thus not subject to the Directive:

- the Data Controller pseudonymises or key-codes Personally Identifiable Data (PID) to be given to a Data Processor that does not receive the key
- the goal of the processing must not be to identify individuals and influence or treat them differently from others.

Pseudonymisation is a Privacy Enhancing Technology (PET), is essentially the replacement of Personally Identifiable Data (PID) – such as name, address or account number – with pseudonyms. Key-coded data are a classical example of pseudonymisation. Personally Identifiable Data (PID) is earmarked by codes, while the link between the code and the PID (like name, date of birth, address, etc.) is kept separately. Pseudonymised data can be used for audits, research, analysis, and administrative tasks or other work that requires access to relationships and trends in the data but not to PID.

Appendix D``

Ref: USB IG .....

Information Governance Assurance

Application for an encrypted USB

To register the requirement for a Trust supplied USB stick enabling secure data flows and transfer of PID, sensitive and confidential information. It is recommended best practice for all Trust dataflows regardless of content to be by encrytpted USB stick
USB sticks should NOT be used for permanent data storage.

Sheffield Teaching Hospitals NHS
NHS Foundation Trust

Department for Information Governance, Caldicott & SIRO Support
Floor 5, Weston Park Hospital
Whitham Road, Sheffield. S10 2SJ
Tel: 0114-2265151 Fax: 0114-2265152
Email: infogov@sth.nhs.uk

Return to the above address on completion

Note: anonymised and pseudonymised data is not PID: see overleaf

1. Name:

2. Designation:

3. Department:

4. Tel/bleep/email:

5. Reason(s) for application

Is the stick to be used on: a) A PC ☐ b) A Mac ☐ c) Both ☐

6. Details of data regularly transferred using the device *(list all that apply)*

7. Have the data flows/transfers been approved? *(PID or similar only)* YES ☐ NO ☐

8. If 7 is yes, who approved the data flows?

9. Have all the data flows/transfers been mapped and registered with IG? YES ☐ NO ☐

Please note: it is Trust policy that all portable electronic storage media such as USB sticks that could contain PID must be encrypted, and the data mapped and registered. All external electronic data flows by e-mail that do contain PID must be encrypted, data mapped and registered, unless sent by NHS-mail to another NHS-mail account when they should be data mapped and registered. Electronic data flows within the Trust network, ie to other internal departments and via internal sth.nhs.uk e-mail to an sth.nhs.uk e-mail address need not be registered. External hard copy data flows of PID should be mapped and registered even if the flow is from campus to campus.
See related Information Governance policies and procedures for further information.

10. If 9 is yes, please supply Data Mapping reference number(s) where appropriate

IGA ..... IGA ..... IGA ..... IGA .....
IGA ..... IGA ..... IGA ..... IGA .....
Continue on a separate sheet if necessary

11. If 9 is no, please complete a Data Mapping Notification Form for each data flow or transfer

Please note: failure to provide details of existing and proposed PID data flows and transfers using the Notification Form could delay or prevent a Trust approved and registered encrypted USB stick being issued. Use of unencrypted USB sticks for the transfer of PID breaches Trust policies and procedures and could lead to disciplinary action.

12. In completing the above information and signing this form, I apply for a Trust encrypted USB stick to be issued for my use under the terms and conditions of the Trust's relevant information security policies and procedures, including Trust mandated 8 digit alpha-numeric passwords as a minimum.
I understand that the stick remains the property of Sheffield Teaching Hospitals NHS Foundation Trust, and must be surrendered in the event that I leave the Trust's employ.

Signed ..... Dated d d m m y y

Information Governance use only:

Form checked and validated by..... Title.....

Stick: issued ☐ refused ☐ Refusal reason.....

Signed..... Dated..... Stick Serial No. **IG**..... Stick Size-2Gb

Anonymised and Pseudonymised Data

Definitions

Anonymised data

Data concerning an individual from which the identity of the individual cannot be determined. The second Caldicott principle is that patient identifiable information should not be used unless absolutely necessary: use anonymised data instead.

In practice, anonymised data should exclude the name, address and full post code, and any other information which when combined with other information likely to be held by or available to the recipent could allow the individual to be identified.

Unique identifiers such as hospital or NHS number should also be excluded if there is any possibility that any recipient of the data has access to the 'key' to that identifier and could thereby trace the identity of the individual.See pseudonymisation, below..

Anonymised and aggregated information can only be used for justified purposes. Staff must ensure that individuals cannot be identified from the information

Pseudonymised Data

The European Commission on Data Protection (DP) has defined pseudonymised data as non-personal data and not subject to the Data Protection Directive in certain instances.

In its “Opinion 4/2007 on the concept of personal data”, the European Commission Article 29 Data Protection Working Party (WP) clarified the notion of "personal data" thus enhancing legal certainty through the uniform interpretation of the EC Directive 95/46/EC. The document describes the following conditions necessary to consider pseudonymised data as non-personal data and thus not subject to the Directive:

- the Data Controller pseudonymises or key-codes Personally Identifiable Data (PID) to be given to a Data Processor that does not receive the key
- the goal of the processing must not be to identify individuals and influence or treat them differently from others.

Pseudonymisation is a Privacy Enhancing Technology (PET), is essentially the replacement of Personally Identifiable Data (PID) – such as name, address or account number – with pseudonyms. Key-coded data are a classical example of pseudonymisation. Personally Identifiable Data (PID) is earmarked by codes, while the link between the code and the PID (like name, date of birth, address, etc.) is kept separately. Pseudonymised data can be used for audits, research, analysis, and administrative tasks or other work that requires access to relationships and trends in the data but not to PID.