THE INFORMATION MAPPING TOOL

GUIDANCE FOR NHS TRUSTS AND GP PRACTICES

[Version 2.6 – 02 July 2009]

The NHS Chief Executive's directives (December 2007 and January 2008) require all NHS organisations to have an up-to-date register of information transfers (i.e. audit or 'map' the flows of information in, out and across the NHS organisation).

The purpose of the NHS CFH Information Mapping Tool is to assist compliance with these directives which support legal and ethical obligations in handling personal and sensitive information.

TABLE OF CONTENTS

BACKGROUND

Why Map Information Flows?

1. In the NHS, numerous urgent and routine transfers of patient and staff information take place each day for the purposes of healthcare and administration of healthcare services e.g. letters to patients, e-mails to job candidates, patient notes made during a home visit, moving case notes.

2. It has long been recognised that this information is more vulnerable to loss or compromise when outside the organisation i.e. being carried around or sent / copied from one location to another. The requirement to map information flows has been included in organisational confidentiality audits since 2001 e.g. Version 6 of the Information Governance Toolkit (IGT) states:

> **NHS Trust** (criterion 208). Has the [organisation] mapped all flows of person identifiable information, assessed risks in line with Department of Health guidelines and put in place safe haven procedures for all routine flows of person identifiable information to the organisation?

3. It also assists with:

> **GP Practice** (criterion 211). Does the Practice ensure that all correspondence, faxes, e-mail, telephone messages, transfer of patient records and other communications are conducted in a secure and confidential manner?

4. Information mapping focuses on these vulnerable areas helping to ensure information is secure in transit.

The Information Mapping Tool

5. The Mapping Tool was developed in 2007 – 2008 by Barts and the London NHS Trust and NHS CFH. The aim of this tool is to assist in systematic and comprehensive mapping of information flows to identify and record risks in the transfer and storage of person identifiable or sensitive information. It provides guidance only and should not be used as the basis for making any business, legal or any other decisions.

6. The Mapping Tool is accessible via the Information Governance Toolkit website. https://www.igt.connectingforhealth.nhs.uk/

Information Mapping Tool Versions – NHS Trust and GP Practice

7. There are currently two versions of the Tool (NHS Trusts and General Practice). Guidance for both versions is contained in this document. The main difference is:

- A GP Practice is classed as a single ‘work area’ with one individual to map information flows, whereas a Trust will identify multiple work areas (departments / directorates) and need to co-ordinate the work of mapping users from each work area

Action on Identifying a Serious Risk

8. If a serious risk is identified (using the Mapping Tool or another method), it is expected that immediate action will be taken to suspend the transfer or amend / replace unacceptable working practices with more secure methods.

9. All risks should be recorded and appropriately reported e.g. to the Senior Information Risk Owner (SIRO), Board, equivalent executive group or Senior Partner to ensure there is an evidence - based approach to decisions making.

10. In circumstances where there is no immediate alternative to continuing the existing practice the action described above should be applied.

11. Guidance on running reports and analysing risk ratings is at Annex E.

Unencrypted Digital Data – Don't Use Post or Courier

12. On 15 January 2008[1] the NHS Chief Executive directed the *immediate suspension* of all transfers by courier or post of unencrypted [digital] data of patient identifiable data (including primary care) unless essential for patient care and:

- *Any unencrypted data transfers that continue should be:*
    - *signed off by the appropriate organisation's Board with a description of how the public will be protected*
    - **notified to the SHA*

- *Any suspended data transfers should be notified to Boards and the *SHA with a plan for how they are to be replaced or made secure*

[GP Practices should report via their PCT]*

The Format of This Document

13. The guidance is set out as:

Annex:

A.	Introduction to Information Mapping	Trusts and GP Practices
B.	Using the Mapping Tool	NHS Trusts
C.	Using the Mapping Tool	GP Practices
D.	Creating Reports	Trusts and GP Practices
E.	Flows That Are High Risk	Trusts and GP Practices

[1] NHS CE letter Gateway ref: 9344 dated 15 Jan 08

ANNEX A - INTRODUCTION TO INFORMATION MAPPING (TRUSTS & GP PRACTICES)

What Is An Information[2] Flow?

1. A transfer of information of information from one location to another. In some organisations the information may stay within the organisation yet a transfer takes place because the department, clinic, branch surgery is located elsewhere (off site). The principle of mapping information flows is to protect information – so if information is transferred between sites, then there will be a higher risk to the information and this transfer should be included.

Overview of the Information Mapping Tool

2. The Information Mapping Tool identifies four elements (for every transfer).

- ***DATA ITEMS*** – the information (which we have a duty to protect) that is being transferred (e.g. a letter contain a single piece of information or a combination e.g. a person's name, address, NHS Number, bank details, medical condition).

Data Item - Patient Notes

Data Item – Patient X-Ray

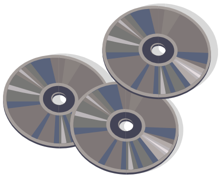
Data Item – Interview Notes

- ***FORMATS*** (e.g. a hardcopy - letter, digital / electronic – computer files, CDs).

Format - Hardcopy Letter

Format - Digital MP3 player

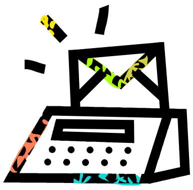
Format - Digital CD



[2] 'Information' and 'Data' are used interchangeably in this document – though 'Information' is often used to denote hard copy records whereas 'data' is more often used to describe digital (electronic / computerised) information. For the purpose of the Mapping Tool there is no distinction made.

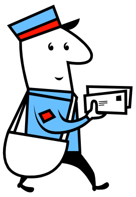
- ***TRANSFER METHODS*** (e.g. post, courier, e-mail).

Transfer Method - Fax



Transfer Method – carried by staff

Transfer Method - Post



- ***LOCATIONS*** of the recipient (e.g. another healthcare organisation, services or offices situated off - site, patient addresses, social services offices).

Location – Patient's Home

Location – Hospital

Location – Equipment Store

3. The Mapping Tool allocates a basic grading of 'High' (RED), 'Medium' (AMBER) or 'Low' (GREEN) to the security assurance afforded by the particular transfer method. This is indicative only.

Generic Locations

4. It is not necessary to give a name to every single location if the same Data Item(s), Format and Transfer Method are used (and therefore the probability of something going wrong is identical for each of these identical transfers) e.g.:

✓ Sending patient appointment letters to patients – there is no need to list each patients' address

✓ Transferring patient records to a local GP Practice – there is no need to name the specific Practice – as long as the transfers to all local Practices involve the same Data Item(s), Format and Transfer Method

5. If this is the case these locations can be listed generically as 'Patient / Carer' or 'GP Practice - Other' (see location / destination paragraphs for more).

Frequency of Transfer

6. To meet the aim of the mapping exercise, all routine (including annual) transfers that take place or are expected to take place should be included in information mapping. This will include irregular and infrequent transfers

What to Include and Exclude?

Included Information

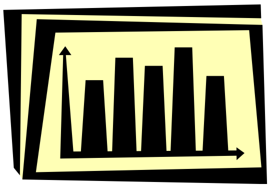
Data Item - Patient Notes

7. All Person Identifiable Data (e.g. patient, client, contractor, staff) supplied with a reasonable expectation of being used in confidence including documents which contain personal data such as employment and other contracts, minutes and agendas from formal committee meetings e.g. assessment panels, case conferences in addition to personnel records, health records, case records, patient notes.

8. Person identifiable data of the deceased (because the NHS duty of confidentiality continues after death).

9. The NHS Number (as it is a unique identifier and is therefore Person Identifiable Data).

Excluded Information



10. Information that poses no security threat because it is:

- × Fully anonymised (including health data statistics)
- × Personal data but no confidentiality restrictions apply e.g. staff names and contact details contained in patient / public information leaflets, newspaper articles, approved versions of public board meetings; annual reports)
- × Already lawfully available in the public domain (e.g. public appointment details, names of staff occupying publicly accountable posts and public facing staff)

Included Formats

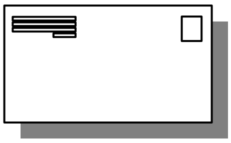
11. Mapping should be carried out on information formats which have physical properties. It could be in hard copy or digital format such as:

Digital e.g.:

- ✓ Computers
- ✓ CDs, DVDs, optical discs
- ✓ Audio and Video tapes
- ✓ Floppy discs
- ✓ Personal Digital Assistants
- ✓ Back up tapes
- ✓ Telephone answering machine messages
- ✓ On-line registration systems
- ✓ Digital Photographs on a Camera
- ✓ SMS Text Message

Hard Copy e.g.:

- ✓ Printed Letters
- ✓ Printed Documents
- ✓ Printed Reports
- ✓ Computer printouts
- ✓ Printed Photographs & Negatives
- ✓ Files
- ✓ X-Rays
- ✓ Microfiche
- ✓ Notepads
- ✓ Diaries
- ✓ P45
- ✓ P60



12. Memory sticks are highly susceptible to loss and the use of these should be closely controlled.

Excluded Formats

13. Information formats that cannot be stored as it does not exist in physical form e.g.:

- × Face to face discussions / briefings
- × Telephone conversations
- × Video / Conference Calls
- × Remote viewing systems (systems designed to hold data centrally, not to copy or transfer physical information) e.g. Patient Administration Systems, Electronic Staff Record, Registration Authority Spine User Directory, Choose and Book, SBS payroll.

14. If discussions are recorded, notes taken or printouts made then this action will create information in digital or hard copy format. Subsequent transfers of the new format may need to be included.

Included Transfer Methods

15. The methods of transfer will include:

- ✓ Email (as this creates local copies)
- ✓ Courier
- ✓ Fax
- ✓ Post
- ✓ Text Message
- ✓ Automatic system transfer
- ✓ Manual upload to system
- ✓ Staff taking information off – site or to a location
- ✓ Hand Delivery by Staff

Excluded Transfer Methods

16. The following may be excluded from information flow mapping (though these transfers methods should be subject to security controls such as IT policies, written procedures and staff awareness sessions):

× Accessing shared drives within the Organisation
× Locally hosted secure systems (which could include DATIX, Ulysses)
× Automated flows between national systems (e.g. Systems and Service Delivery (formerly NHAIS), Secure File Transfers)
× National e-learning applications (user registration details)
× National NHS applications (e.g. Choose and Book, Secondary Uses Service)
× Automated flows between local systems (e.g. Patient Administration System sub systems)

Included Locations / Organisation Areas

17. All transfers that take place or are expected to take place:

✓ In or out of the Organisation
✓ Between departments on separate sites within the Organisation

18. This includes transfers to NHS organisations, courts, solicitors, insurance companies, disposal[3] sites, storage, archives, Independent Sector Treatment Centres (ISTCs), information sharing partnership organisations, patients (letters, Data Protection Act Subject Access Requests (SARs) etc). Transfers between departments are included as these may be on different sites or deal with high volumes of transfers.

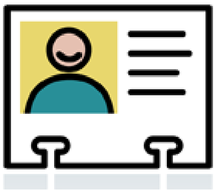
Excluded Locations / Organisation Areas

19. The following can be excluded:

× Transfers between health professionals in the same building / location e.g. patient notes or health records during normal episodes of care
× Unforeseen and unexpected transfers (though security measures will still apply)
× Collections (rather than transfers) of information copied within the same department for referencing purposes. NB Staff should not collate and store collections of information which contains Person Identifiable Data for personal reference

[3] Including transfers to off site disposal should also be included e.g. disposal of computer hard drives and other electronic media which may have previously stored personal identifiable data which has not been fully and irreversibly deleted.

What Is Personal Identifiable Data?



20. Personal Identifiable Data (PID) is information (an identifier) about a person e.g. a patient, client, service user or staff, from which the individual could be singled out from others. It may be a single or combination of two or more identifiers such as:

- ✓ Name
- ✓ Address (home or business)
- ✓ Postcode (e.g. a house in rural area)
- ✓ NHS No
- ✓ Email address
- ✓ Date of birth
- ✓ Driving licence number (date of birth and first part of surname)
- ✓ Telephone numbers
- ✓ Local Patient Identifier
- ✓ National Insurance No

21. A single identifier may be fairly explicit such as an unusual surname, an isolated postcode or combination such as of postcode and telephone number.

What Personal Information Needs Protection?

22. This depends upon the individual, nature, source and extent of the information already available. As a guide, the NHS defines the minimum scope of Protected Personal Data as that which falls into one (or both) of the categories (A, B) shown in the table at Appendix 1. This is a guide only as organisations need to determine whether other information they hold would be more suitable in whichever category e.g. persons whose personal data may be of greater sensitivity – senior politicians, publicly known figures. The table gives examples of:

- **Category A**. Personal Data (individual identifiers) which may lead to identification of an individual and his / her associated Sensitive Personal Data. This data requires protection due to the potential adverse impact on an individual and / or the organisation e.g. public confidence in the public service provider.

- **Category B**. Personal Data (individual identifiers) of 51 individuals which will not lead to identification of the individual and their associated Sensitive Personal Data. This data requires protection due to the potential adverse impact on the group of individuals and / or the organisation e.g. public confidence in the public service provider.

23. The table at Appendix 1 lists Category A and Category B Personal Data in more detail.

What Is Bulk Personal Identifiable Data?

24. The term ‘bulk’ is used to describe information relating to 51 or more individuals. This may be Category A (sensitive) or B (non – sensitive).

Prioritising the Mapping Exercise

25. To ensure high risk areas are addressed in timely manner it is recommended that the flows which routinely generate a high volume of personal identifiable information are addressed as priority e.g. bulk data and those that contain sensitive data, clinical departments dealing with patient information, Payroll, Human Resources.

Who Should Be Involved In Information Mapping?

Smaller Organisations e.g. a GP Practice

26. Assuming that a Practice equates to a Trust directorate or department, mapping may be best suited to one individual with the required in-depth knowledge of the working practices.

Large Organisations e.g. a Trust

27. One individual will not have the knowledge required to comprehensively and accurately map flows throughout each directorate, department and service of a large or geographically dispersed organisation.

28. Those staff who are responsible for, and employed in, the relevant work areas should be involved in the mapping exercise to ensure a full and complete picture is obtained and awareness and importance of secure working practices and procedures is reinforced.

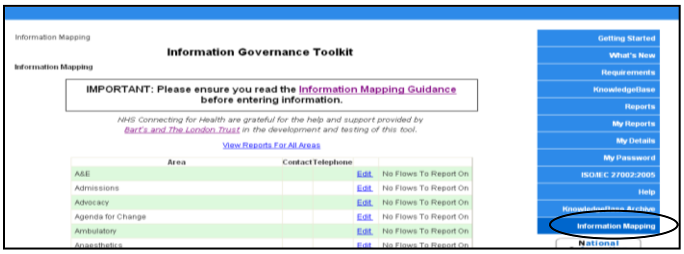
Mapping Tool Key Terms

29. The Tool is designed to allow administrators to define and input the organisation’s work areas, data items and the locations to which the data is sent. The users may then populate the Tool with the transfers taking place. Following partial or total completion of the toolkit, reports may be created highlighting the results by area or organisation. The key elements are shown below:

- **Users and Administrators** - The staff who will complete the audit and create additional Areas, Items and Locations as needed.
- **Areas** (NHS Trusts only) - Departments and other work areas in your Trust (the most common are already listed to choose from) e.g. post room, HR dept. **GP Practices are assumed to be a single area – so this option does not appear in the GP Version.**
- **Data Items** - the piece of person identifiable or other sensitive information being transferred e.g. job application forms, staff bank details form or a patient appointment letter.
- **Locations** - an external organisation (or destination) which an organisation sends information to or receives information from e.g. GP Practice, Acute Hospital, Social Services.

Help and Example Materials

30. Select the **Information Mapping** option on the bottom right-hand side of the screen.



Information Mapping

Information Governance Toolkit

Information Mapping

IMPORTANT: Please ensure you read the Information Mapping Guidance before entering information.

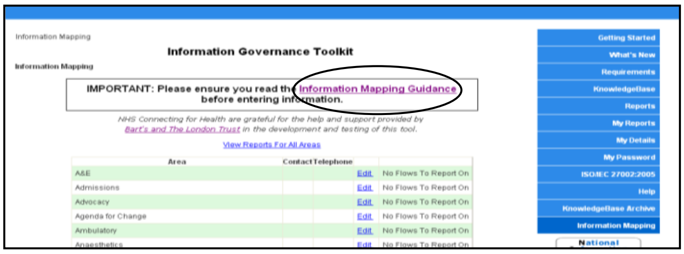
NHS Connecting for Health are grateful for the help and support provided by Bart's and The London Trust in the development and testing of this tool.

View Reports For All Areas

Area	Contact	Telephone		
A&E			Edit	No Flows To Report On
Admissions			Edit	No Flows To Report On
Advocacy			Edit	No Flows To Report On
Agenda for Change			Edit	No Flows To Report On
Ambulatory			Edit	No Flows To Report On
Anaesthetics			Edit	No Flows To Report On

31. Click the **Information Mapping Guidance** link at the top of the page.

- Select from the list of guidance materials provided (click on links to open the documents).



Information Mapping

Information Governance Toolkit

Information Mapping

IMPORTANT: Please ensure you read the Information Mapping Guidance before entering information.

NHS Connecting for Health are grateful for the help and support provided by Bart's and The London Trust in the development and testing of this tool.

View Reports For All Areas

Area	Contact	Telephone		
A&E			Edit	No Flows To Report On
Admissions			Edit	No Flows To Report On
Advocacy			Edit	No Flows To Report On
Agenda for Change			Edit	No Flows To Report On
Ambulatory			Edit	No Flows To Report On
Anaesthetics			Edit	No Flows To Report On

Appendices:

1. Table 1: Category A – (Individual) Sensitive Personal Data and Category B (Group) Personal Data.
2. Member States of the European Economic Area.

APPENDIX 1 TO ANNEX A

Table 1: Protected Personal Data Categories A & B

Category A • Personal Data (column (a)) which can be combined with other, already available, information to identify an individual's sensitive personal data (column (b) OR • Sensitive Personal Data (column (b))		
(a)		(b)
Personal Data (Individual Identifiable)		**Sensitive Personal Data (Individual Identifiable)**
A non-sensitive identifier, the disclosure of which, is unlikely to cause damage or distress to an individual or third party (exemptions apply).		Information, the disclosure of which, is likely to cause damage or distress to an individual or third party e.g.:
Defined in the Data Protection Act as: Data relating to a *living* individual who can be identified; • from those data (e.g. an employee's name), or • from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller (e.g. an employee's payroll number) For NHS common law duty of confidence purposes, Individual Identifiers / Personal Identifiable Data also applies to *deceased* patients. This information includes single items such as: • Name • Address (home or business) • Postcode • NHS No • Email address • Date of birth • Payroll number • Driving Licence [shows date of birth and first part of surname]		**Defined by the Data Protection Act as:** Personal Data consisting of information as to: • Racial / ethnic origin • Political opinions • Religious beliefs • Trade union membership • Physical or mental health • Sexual life • Criminal offences AND …for Information mapping purposes will include information which may lead to damage or distress (e.g. breach of privacy, financial loss) such as: • Biometrics; DNA Profile, Fingerprints • Bank, Financial Or Credit Card Details • Mother's Maiden Name • National Insurance Number • Tax, Benefit Or Pension Records • Health, Adoption, Employment, School, Social Services, Housing Records • Child Protection
Category B Personal Data (not in the public domain) of 51* or more individuals, the disclosure of which is unlikely to cause an individual damage or distress but would harm public confidence		
(a)	(b)	(c)
A database, electronic folder, disk, or paper records of patients' names and addresses.		**Not Applicable**

* The number of 51 is a minimum standard for aggregated information of a non – sensitive nature relating to individuals. Personal Data (Individual Identifiers) on smaller numbers of individuals may warrant protection because of the nature of the individuals, nature, source or extent of the information.

**APPENDIX 2 TO
ANNEX A**

Member States of the European Economic Area

Austria	Greece	Netherlands
Belgium	Hungary	_*Norway_
Bulgaria	_*Iceland_	Poland
Republic of Cyprus	Ireland	Portugal
Czech Republic	Italy	Romania
Denmark	Latvia	Slovakia
Estonia	_*Liechtenstein_	Slovenia
Finland	Lithuania	Spain
France	Luxembourg	Sweden
Germany	Malta	United Kingdom

* Iceland, Liechtenstein and Norway are EEA member states, but they are not members of the European Union (EU).